

JP 01/772

EU

日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT

PCT/JP01/00772

02.02.01

#4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年12月 5日

出願番号

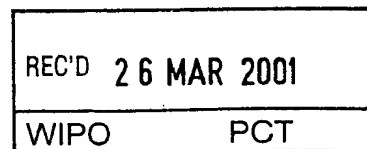
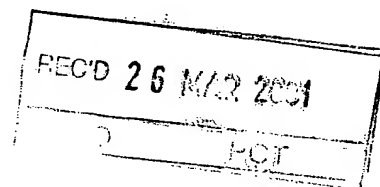
Application Number:

特願2000-370519

出願人

Applicant(s):

ソニー株式会社



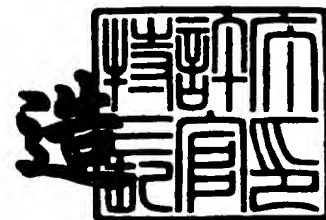
09/937797

**PRIORITY  
DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 3月 2日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2001-3015201

【書類名】 特許願

【整理番号】 0000763125

【提出日】 平成12年12月 5日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 金巻 裕史

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 佐竹 清

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 齋藤 真

【発明者】

    【住所又は居所】 東京都中央区日本橋室町1丁目6番地3号 ソニーケミ  
                                カル株式会社内

    【氏名】 中村 嘉秀

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 橋本 主税

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【先の出願に基づく優先権主張】

【出願番号】 特願2000- 24619

【出願日】 平成12年 2月 2日

【先の出願に基づく優先権主張】

【出願番号】 特願2000-209674

【出願日】 平成12年 7月11日

【先の出願に基づく優先権主張】

【出願番号】 特願2000-209675

【出願日】 平成12年 7月11日

【先の出願に基づく優先権主張】

【出願番号】 特願2000-234741

【出願日】 平成12年 8月 2日

【先の出願に基づく優先権主張】

【出願番号】 特願2000-234752

【出願日】 平成12年 8月 2日

【先の出願に基づく優先権主張】

【出願番号】 特願2000-238077

【出願日】 平成12年 8月 7日

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

特 2 0 0 0 - 3 7 0 5 1 9

【包括委任状番号】 9707389

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 認証装置、認証システムおよびその方法、処理装置、通信装置、通信制御装置、通信システムおよびその方法、情報記録方法およびその装置、情報復元方法およびその装置、並びに記録媒体

【特許請求の範囲】

【請求項 1】

ネットワークを介して少なくとも 2 者間で行われる取引きを認証する認証装置において、

第 1 の取引き者の個人識別情報、第 2 の取引き者の個人識別情報および取引き内容を示す情報を含む第 1 の要求を、前記第 1 の取引き者から受信する第 1 の受信手段と、

前記第 1 の要求に応じて、前記第 1 の取引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、

前記第 1 の認証情報および前記取引きの内容を示す情報を含む第 2 の要求を前記第 2 の取引き者に送信する第 1 の送信手段と、

前記第 2 の要求に対しての応答を前記第 2 の取引き者から受信する第 2 の受信手段と、

前記応答に応じて、前記第 2 の取引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、

前記第 2 の認証情報を前記第 1 の取引き者に送信する第 2 の送信手段とを有する認証装置。

【請求項 2】

前記第 1 の受信手段は、前記第 1 の取引き者の個人キー情報をさらに含む前記第 1 の要求を受信し、

前記第 1 の認証手段は、前記個人キー情報に基づいて前記第 1 の取引き者の正当性を認証し、

前記第 2 の受信手段は、前記第 2 の取引き者の個人キー情報を含む前記応答を受信し、

前記第 1 の認証手段は、前記第 2 の取引き者の個人キー情報に基づいて前記

第 2 の取り引き者の正当性を認証する

請求項 1 に記載の認証装置。

【請求項 3】

前記第 1 の取り引き者および前記第 2 の取り引き者の前記個人キー情報は、それぞれ前記第 1 の取り引き者および前記第 2 の取り引き者の課金に係わる情報である

請求項 2 に記載の認証装置。

【請求項 4】

前記第 1 の送信手段は、前記第 1 の取り引き者の前記個人キー情報をさらに含む第 2 の要求を前記第 2 の取り引き者に送信する

請求項 3 に記載の認証装置。

【請求項 5】

前記取り引きの履歴を示す履歴情報を記憶する記憶手段  
をさらに有する請求項 1 に記載の認証装置。

【請求項 6】

前記第 1 の要求が暗号化されている場合に、前記受信した第 1 の要求を復号する復号手段

をさらに有する請求項 1 に記載の認証装置。

【請求項 7】

前記第 2 の要求を暗号化する暗号化手段  
をさらに有する請求項 1 に記載の認証装置。

【請求項 8】

前記応答が暗号化されている場合に、前記受信した応答を復号する復号手段  
をさらに有する請求項 1 に記載の認証装置。

【請求項 9】

前記第 2 の認証情報を暗号化する暗号化手段  
をさらに有する請求項 1 に記載の認証装置。

【請求項 10】

ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証シ

システムにおいて、

第1の取引引き者が使用する第1の通信装置と、

第2の取引引き者が使用する第2の通信装置と、

前記取引引きを認証する認証装置と

を有し、

前記第1の通信装置は、第1の取引引き者の個人識別情報、第2の取引引き者の個人識別情報および取引引き内容を示す情報を含む第1の要求を前記認証装置に送信し、

前記認証装置は、

前記第1の取引引き者から前記第1の要求を受信する第1の受信手段と、

前記第1の要求に応じて、前記第1の取引引き者の正当性を認証して第1の認証情報を生成する第1の認証手段と、

前記第1の認証情報および前記取引引きの内容を示す情報を含む第2の要求を前記第2の取引引き者に送信する第1の送信手段と、

前記第2の要求に対しての応答を前記第2の取引引き者から受信する第2の受信手段と、

前記応答に応じて、前記第2の取引引き者の正当性を認証して第2の認証情報を生成する第2の認証手段と、

前記第2の認証情報を前記第1の取引引き者に送信する第2の送信手段と

を有する

認証システム。

#### 【請求項11】

前記第1の受信手段は、前記第1の取引引き者の個人キー情報をさらに含む前記第1の要求を受信し、

前記第1の認証手段は、前記個人キー情報に基づいて前記第1の取引引き者の正当性を認証し、

前記第2の受信手段は、前記第2の取引引き者の個人キー情報を含む前記応答を受信し、

前記第1の認証手段は、前記第2の取引引き者の個人キー情報に基づいて前記

第2の取引引き者の正当性を認証する

請求項10に記載の認証システム。

【請求項12】

前記第1の取引引き者および前記第2の取引引き者の前記個人キー情報は、それぞれ前記第1の取引引き者および前記第2の取引引き者の課金に係わる情報である

請求項11に記載の認証システム。

【請求項13】

ネットワークを介して少なくとも2者間で行われる取引引きを認証する認証方法において、

第1の取引引き者の個人識別情報、第2の取引引き者の個人識別情報および取引引き内容を示す情報を含む第1の要求を、前記第1の取引引き者から受信し、

前記第1の要求に応じて、前記第1の取引引き者の正当性を認証して第1の認証情報を生成し、

前記第1の認証情報および前記取引引きの内容を示す情報を含む第2の要求を前記第2の取引引き者に送信し、

前記第2の要求に対しての応答を前記第2の取引引き者から受信し、

前記応答に応じて、前記第2の取引引き者の正当性を認証して第2の認証情報を生成し、

前記第2の認証情報を前記第1の取引引き者に送信する

認証方法。

【請求項14】

前記第1の取引引き者の個人キー情報をさらに含む前記第1の要求を受信し、

前記個人キー情報に基づいて前記第1の取引引き者の正当性を認証し、

前記第2の取引引き者の個人キー情報を含む前記応答を受信し、

前記第2の取引引き者の個人キー情報に基づいて前記第2の取引引き者の正当性を認証する

請求項13に記載の認証方法。

【請求項15】

前記第1の取引引き者および前記第2の取引引き者の前記個人キー情報は、それぞれ前記第1の取引引き者および前記第2の取引引き者の課金に係わる情報である

請求項14に記載の認証方法。

【請求項16】

前記第1の取引引き者の前記個人キー情報をさらに含む第2の要求を前記第2の取引引き者に送信する

請求項15に記載の認証方法。

【請求項17】

前記第2の取引引き者は、前記第1の取引引き者の個人キー情報を用いて決済を行う

請求項16に記載の認証方法。

【請求項18】

ネットワークを介して少なくとも2者間で行われる取引引きを認証する認証装置において、

第1の取引引き者の個人識別情報、前記第1の取引引き者の個人キー情報、第2の取引引き者の個人識別情報および取引引き内容を示す情報を含む第1の要求を、前記第1の取引引き者から受信する第1の受信手段と、

前記第1の要求に含まれる前記個人キー情報に基づいて前記第1の取引引き者の正当性を認証して第1の認証情報を生成する第1の認証手段と、

前記第1の要求から前記第1の取引引き者の個人キー情報を除去した情報と、前記第1の認証情報とを含む第2の要求を前記第2の取引引き者に送信する第1の送信手段と、

前記第2の要求に対しての応答を前記第2の取引引き者から受信する第2の受信手段と、

前記応答に応じて、前記第2の取引引き者の正当性を認証して第2の認証情報を生成する第2の認証手段と、

前記第2の認証情報を前記第1の取引引き者に送信する第2の送信手段とを有する認証装置。

【請求項 1 9】

前記第 2 の受信手段は、前記第 2 の取り引き者の個人キー情報を含む前記応答を受信し、

前記第 1 の認証手段は、前記第 2 の取り引き者の個人キー情報に基づいて前記第 2 の取り引き者の正当性を認証する

請求項 1 8 に記載の認証装置。

【請求項 2 0】

前記第 1 の取り引き者の個人キー情報は前記第 1 の取り引き者の課金に係わる情報であり、前記第 2 の取り引き者の個人キー情報は前記第 2 の取り引き者の課金に係わる情報である

請求項 1 9 に記載の認証装置。

【請求項 2 1】

前記取り引きの履歴を示す履歴情報を記憶する記憶手段

をさらに有する請求項 1 8 に記載の認証装置。

【請求項 2 2】

ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証システムにおいて、

第 1 の取り引き者が使用する第 1 の通信装置と、

第 2 の取り引き者が使用する第 2 の通信装置と、

前記取り引きを認証する認証装置と

を有し、

前記認証装置は、

第 1 の取り引き者の個人識別情報、前記第 1 の取り引き者の個人キー情報、第 2 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、

前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、

前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信する第 1

の送信手段と、

前記第2の要求に対しての応答を前記第2の取り引き者から受信する第2の受信手段と、

前記応答に応じて、前記第2の取り引き者の正当性を認証して第2の認証情報を生成する第2の認証手段と、

前記第2の認証情報を前記第1の取り引き者に送信する第2の送信手段と

を有する

認証システム。

#### 【請求項23】

ネットワークを介して少なくとも2者間で行われる取り引きを認証する認証方法において、

第1の取り引き者の個人識別情報、前記第1の取り引き者の個人キー情報、第2の取り引き者の個人識別情報および取り引き内容を示す情報を含む第1の要求を、前記第1の取り引き者から受信し、

前記第1の要求に含まれる前記個人キー情報に基づいて前記第1の取り引き者の正当性を認証して第1の認証情報を生成し、

前記第1の要求から前記第1の取り引き者の個人キー情報を除去した情報と、前記第1の認証情報とを含む第2の要求を前記第2の取り引き者に送信し、

前記第2の要求に対しての応答を前記第2の取り引き者から受信し、

前記応答に応じて、前記第2の取り引き者の正当性を認証して第2の認証情報を生成し、

前記第2の認証情報を前記第1の取り引き者に送信する

認証方法。

#### 【請求項24】

前記第1の取り引き者の個人キー情報を用いて、前記取り引きの決済を行う請求項23に記載の認証方法。

#### 【請求項25】

認証要求に応じて認証処理を行う認証装置であって、

利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別

する装置識別情報とを含む前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段と

を有する認証装置。

【請求項 2 6】

前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段

をさらに有する請求項 2 5 に記載の認証装置。

【請求項 2 7】

前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する

請求項 2 5 に記載の認証装置。

【請求項 2 8】

前記個人識別情報は、登録した利用者に予め割り当てられた識別子である

請求項 2 5 に記載の認証装置。

【請求項 2 9】

前記装置識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である

請求項 2 5 に記載の認証装置。

【請求項 3 0】

ネットワークを介して行われる取引に関する認証処理を行う認証装置であ



って、

利用者を識別するための個人識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取り引きを行う利用者による前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記受信した認証要求に含まれる前記取り引き情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段と

を有する認証装置。

#### 【請求項 3 1】

前記認証処理手段は、

前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する

請求項 3 0 に記載の認証装置。

#### 【請求項 3 2】

前記記憶手段は、

前記認証要求を発した利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する

請求項 3 0 に記載の認証装置。

#### 【請求項 3 3】

前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、

前記認証装置は、

前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段

をさらに有する請求項 30 に記載の認証装置。

【請求項 34】

前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する

請求項 30 に記載の認証装置。

【請求項 35】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段

をさらに有する請求項 30 に記載の認証装置。

【請求項 36】

ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、

利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む前記認証要求を送信する送信手段と、

認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、

前記装置識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段と

を有する処理装置。

【請求項 37】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項 36 に記載の処理装置。

【請求項 38】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 36 に記載の処理装置。

【請求項 3 9】

ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、

前記認証装置は、

利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、

前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記認証要求に応じて認証処理を行う認証処理手段と、

前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信する送信手段と

を有し、

前記処理装置は、

前記個人識別情報と、当該処理装置を識別するための前記装置識別情報とを含む前記認証要求を送信する送信手段と、

前記認証応答を受信する受信手段と、

当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する制御手段と

を有する

認証システム。

【請求項 4 0】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する

請求項 3 9 に記載の認証システム。

【請求項 4 1】

前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引き先の装置

に所定の通知を行う

請求項 3 9 に記載の認証システム。

【請求項 4 2】

ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、

利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、

前記認証装置において前記認証要求に応じて認証処理を行い、

前記認証装置から、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信し、

前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記装置識別情報と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する

認証方法。

【請求項 4 3】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証装置に通知する

請求項 4 2 に記載の認証方法。

【請求項 4 4】

前記処理装置は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取引先先の装置に所定の通知を行う

請求項 4 2 に記載の認証方法。

【請求項 4 5】

第 1 の取引引き者に関する情報を保持し、第 2 の取引引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第 1 の取引引き者と前記第 2 の取引引き者との間の取引引きに関する認証を行う認証装置であって、

前記取り引き内容を示す情報と前記第2の取り引き者を特定する情報とを含む前記第1の取り引き者からの第1の要求に応じて、前記第2の取り引き者を特定する情報を含む第2の要求を前記第2の認証装置に送信し、前記第2の要求に応じた前記第2の認証装置による認証結果を示す第1の署名情報を受信し、前記第1の要求に含まれる前記取り引き内容に関する情報と前記第1の署名情報とを含む第3の要求を前記第2の取り引き者が使用する装置に送信し、当該第3の要求に応じて前記第2の取り引き者が使用する装置から所定の応答を受ける送受信手段と、

前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、

前記所定の応答を受けた場合に、前記送受信手段を介して前記第1の取り引き者が使用する装置に送信される第2の署名情報であって、前記取り引きの正当性の認証結果を示す第2の署名情報を作成する署名作成手段と

を有する認証装置。

【請求項46】

暗号化手段

をさらに有し、

前記送受信手段は、前記第2の取り引き者との間の通信に用いる暗号鍵を前記第2の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第1の署名情報とを、前記第2の取り引き者が使用する装置に送信する

請求項45に記載の認証装置。

【請求項47】

前記送受信手段は、

前記他の認証装置が前記第2の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第2の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項45に記載の認証装置。

【請求項48】

前記送受信手段は、前記第1の要求に含まれる前記取り引き内容に関する情報のうち、前記第1の取り引き者の課金に係わる情報以外の情報と、前記第1の署名情報とを含む第3の要求を前記第2の取り引き者が使用する装置に送信する請求項45に記載の認証装置。

【請求項49】

前記送受信手段は、前記第1の要求に含まれる前記取り引き内容に関する情報と、前記第1の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第3の要求を前記第2の取り引き者が使用する装置に送信する

請求項45に記載の認証装置。

【請求項50】

前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する請求項45に記載の認証装置。

【請求項51】

前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項50に記載の認証装置。

【請求項52】

前記送受信手段は、前記第2の取り引き者が前記第1の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第2の取り引き者が使用する装置から、前記記所定の応答を受ける

請求項45に記載の認証装置。

【請求項53】

前記送受信手段は、

前記第2の署名情報を前記第2の取り引き者が使用する装置に送信する

請求項45に記載の認証装置。

【請求項54】

ネットワークを介して少なくとも2者間で行われた取り引きを認証する認証システムにおいて、

第1の取り引き者に関する取り引きを認証する第1の認証装置と、

第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置と  
を有し、

前記第 1 の認証装置は、

前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む  
前記第 1 の取り引き者による第 1 の要求に応じて、前記第 2 の取り引き者を特定  
する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応  
じた前記第 2 の認証装置による認証結果である第 1 の署名情報を受信し、前記第  
1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含  
む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求  
に応じて前記第 2 の取り引き者から所定の応答を受けると、前記取り引きの履歴  
を記憶し、前記取り引きの正当性の認証結果を示す第 2 の署名情報を前記第 1 の  
取り引き者に提供する

認証システム。

【請求項 5 5】

前記第 1 の認証装置は、

暗号化手段

をさらに有し、

前記送受信手段は、前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記  
第 2 の要求に応じて前記第 2 の認証装置から受信し、前記暗号化手段で前記暗号  
鍵を用いて暗号化された前記取り引き内容に関する情報と前記第 1 の署名情報と  
を、前記第 2 の取り引き者が使用する装置に送信する

請求項 5 4 に記載の認証システム。

【請求項 5 6】

前記第 1 の認証装置の前記送受信手段は、

前記第 2 の認証装置が前記第 2 の取り引き者を識別するために用いる識別情報  
を含む前記所定の応答を前記第 2 の取り引き者が使用する装置から受け、

前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶  
する

請求項 5 4 に記載の認証システム。

【請求項 5 7】

前記第 1 の認証装置は、  
前記第 2 の署名情報を前記第 2 の取引引き者に提供する  
請求項 5 4 に記載の認証システム。

【請求項 5 8】

第 1 の取引引き者に関する取引引きを認証する第 1 の認証装置と、第 2 の取引引き者に関する取引引きを認証する第 2 の認証装置とを用いて、ネットワークを介して行われる前記第 1 の取引引き者と前記第 2 の取引引き者との間の取引引きに関する認証を行う認証方法であって、

前記第 1 の取引引き者から前記第 1 の認証装置に、前記取引引き内容を示す情報と前記第 2 の取引引き者を特定する情報とを含む第 1 の要求を出し、

前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 2 の取引引き者を特定する情報を含む第 2 の要求を送信し、

前記第 2 の要求に応じて、前記第 2 の認証装置からの前記第 1 の認証装置に、当該第 2 の認証装置による認証結果を示す第 1 の署名情報を送信し、

前記第 1 の認証装置から前記第 2 の取引引き者が使用する装置に、前記第 1 の要求に含まれる前記取引引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を送信し、

当該第 3 の要求に応じて、前記第 2 の取引引き者が使用する装置から前記第 1 の認証装置に所定の応答を出し、

前記所定の応答に応じて、前記第 1 の認証装置は、前記取引引きの履歴を記憶し、前記取引引きの正当性の認証結果を示す第 2 の署名情報を作成し、当該第 2 の署名情報を、前記第 1 の取引引き者が使用する装置に送信する

認証方法。

【請求項 5 9】

前記第 2 の取引引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて、前記第 2 の認証装置から前記第 1 の認証装置に送信し、

前記第 1 の認証装置は、前記取引引き内容に関する情報と前記第 1 の署名情報とを、前記暗号鍵を用いて暗号化した後に、前記第 2 の取引引き者が使用する装



置に送信する

請求項 5 8 に記載の認証方法。

【請求項 6 0】

前記第 1 の認証装置は、前記第 2 の認証装置が前記第 2 の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第 2 の取り引き者が使用する装置から受け、前記識別情報を用いて生成された前記取り引きの履歴を記憶する

請求項 5 8 に記載の認証方法。

【請求項 6 1】

前記第 1 の要求に含まれる前記取り引き内容に関する情報のうち、前記第 1 の取り引き者の課金に係わる情報以外の情報と、前記第 1 の署名情報とを含む第 3 の要求を、前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に送信する

請求項 5 8 に記載の認証方法。

【請求項 6 2】

前記第 1 の要求に含まれる前記取り引き内容に関する情報と、前記第 1 の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第 3 の要求を、前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に送信する

請求項 5 8 に記載の認証方法。

【請求項 6 3】

前記第 1 の認証装置と前記第 2 の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う

請求項 5 8 に記載の認証方法。

【請求項 6 4】

前記第 2 の取り引き者が前記第 1 の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第 2 の取り引き者が使用する装置から前記第 1 の認証装置に、前記所定の応答を出す

請求項 5 8 に記載の認証方法。

【請求項 6 5】

前記第 1 の認証装置から前記第 2 の取り引き者が使用する装置に、前記第 2 の署名情報を送信する

請求項 5 8 に記載の認証方法。

【請求項 6 6】

利用者を識別するための個人識別情報を含む要求を受信する受信手段と、  
前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段と

を有する通信装置。

【請求項 6 7】

前記受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、

前記通信装置は、

前記受信した要求に含まれる前記個人識別情報を復号する復号手段

をさらに有する請求項 6 6 に記載の通信装置。

【請求項 6 8】

前記個人識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である

請求項 6 6 に記載の通信装置。

【請求項 6 9】

前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である

請求項 6 6 に記載の通信装置。

【請求項 7 0】

前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である

請求項 6 6 に記載の通信装置。

【請求項 7 1】

前記処理は、認証処理である

請求項 6 6 に記載の通信装置。

【請求項 7 2】

ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を有する通信システムであって、

前記第 1 の通信装置は、

利用者を識別するための個人識別情報を含む要求を受信する第 1 の受信手段と

前記個人識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第 1 の送信手段と

を有し、

前記第 2 の通信装置は、

前記要求を前記第 1 の通信装置に送信する第 2 の送信手段と、

前記処理の結果を前記第 1 の通信装置から受信する第 2 の受信手段と、

当該受信した認証処理の結果を出力する出力手段と

を有する

通信システム。

【請求項 7 3】

前記第 1 の通信装置の前記第 1 の受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、

前記第 1 の通信装置は、

前記受信した要求に含まれる前記個人識別情報を復号する復号手段

をさらに有する請求項 7 2 に記載の通信システム。

【請求項 7 4】

前記個人識別情報は、当該第 1 の通信装置に登録された利用者に予め割り当てられた識別子である

請求項 7 2 に記載の通信システム。

【請求項 7 5】

前記処理の結果を送信する送信先の情報は、前記第 2 の通信装置の利用者がオンラインで当該第 1 の通信装置に提供した情報である

請求項 7 2 に記載の通信システム。

【請求項 7 6】

前記処理の結果を送信する送信先の情報は、前記第 1 の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である  
請求項 7 2 に記載の通信システム。

【請求項 7 7】

ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を用いた通信方法であって、

利用者を識別するための個人識別情報を含む要求を、前記第 2 の通信装置から前記第 1 の通信装置に送信し、

前記第 1 の通信装置において、前記要求に応じて所定の処理を行い、

前記第 1 の通信装置は、予め用意された前記個人識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記個人識別情報に対応する送信先の情報によって特定される送信先に、前記処理の結果を送信する

通信方法。

【請求項 7 8】

前記第 2 の通信装置において前記第 1 の通信装置から受信した前記処理の結果を出力する

請求項 7 7 に記載の通信方法。

【請求項 7 9】

前記第 1 の通信装置は、暗号化された前記個人識別情報を含む前記要求を受信し、当該受信した要求に含まれる前記個人識別情報を復号する

請求項 7 7 に記載の通信方法。

【請求項 8 0】

前記個人識別情報は、当該第 1 の通信装置に登録された利用者に予め割り当てられた識別子である

請求項 7 7 に記載の通信方法。

【請求項 8 1】

前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該第 1 の通信装置に提供した情報である

請求項 7 7 に記載の通信方法。

【請求項 8 2】

前記処理の結果を送信する送信先の情報は、前記第 1 の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である  
請求項 7 7 に記載の通信方法。

【請求項 8 3】

単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を制御する通信制御装置であって、

前記第 1 の通信装置を識別するための装置識別情報を記憶する記憶手段と、

前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報を含む要求を前記第 2 の通信装置に送信する送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する受信手段と、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段と

を有する通信制御装置。

【請求項 8 4】

前記制御手段は、

前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識

別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う

請求項 8 3 に記載の通信制御装置。

【請求項 8 5】

前記制御手段は、

前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 8 3 に記載の通信制御装置。

【請求項 8 6】

前記送信手段は、

前記第 1 の通信装置から受信した個人識別情報と、当該第 1 の通信装置に対応する前記装置識別情報とを含む前記要求を前記第 2 の通信装置に送信する

請求項 8 3 に記載の通信制御装置。

【請求項 8 7】

前記記憶手段は、

前記第 1 の通信装置から受信した前記装置識別情報を記憶する

請求項 8 3 に記載の通信制御装置。

【請求項 8 8】

前記記憶手段は、

当該通信制御装置の電源が投入されたときに前記第 1 の通信装置から受信した前記装置識別情報を記憶する

請求項 8 7 に記載の通信制御装置。

【請求項 8 9】

前記制御手段は、

前記第 1 の通信装置と前記第 2 の通信装置との間の通信履歴を前記記憶手段に書き込む

請求項 8 3 に記載の通信制御装置。

【請求項 9 0】

前記制御手段は、

前記応答に含まれる前記第 2 の通信装置の処理結果を、前記要求の送信元の前記第 1 の通信装置に送信する

請求項 8 3 に記載の通信制御装置。

【請求項 9 1】

前記制御手段は、

前記受信手段から受信した情報に応じて、待機状態にある前記第 1 の通信装置が動作状態になるように制御する

請求項 8 3 に記載の通信制御装置。

【請求項 9 2】

前記制御手段は、

前記第 1 の通信装置が接続されたネットワークと、前記第 2 の通信装置が接続されたネットワークとの間の通信を制御する

請求項 8 3 に記載の通信制御装置。

【請求項 9 3】

前記制御手段は、

ゲートウェイとしての処理を行う

請求項 9 2 に記載の通信制御装置。

【請求項 9 4】

前記装置識別情報は、前記第 1 の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である

請求項 8 3 に記載の通信制御装置。

【請求項 9 5】

前記個人識別情報は、登録した利用者に予め割り当てられた識別子である

請求項 8 6 に記載の通信制御装置。

【請求項 9 6】

前記受信手段は、

前記第 2 の通信装置が行った認証処理の結果を含む前記応答を前記第 2 の通信装置から受信する

請求項 8 3 に記載の通信制御装置。

【請求項 9 7】

単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、

前記通信制御装置は、

前記第 1 の通信装置を識別するための装置識別情報を記憶する第 1 の記憶手段と、

前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報と個人識別情報とを含む要求を前記第 2 の通信装置に送信する第 1 の送信手段と、

前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する第 1 の受信手段と、

前記応答に含まれる前記装置識別情報と前記第 1 の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第 1 の記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段と

を有し、

前記第 2 の通信装置は、

前記要求を受信する第 2 の受信手段と、

前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第 2 の記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記第 2 の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第 2 の送信手段と

を有する

通信システム。

【請求項 9 8】



単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、

前記第 1 の通信装置から前記通信制御装置に出された要求に応じて、当該第 1 の通信装置に対応する装置識別情報と個人識別情報とを含む要求を前記通信制御装置から前記第 2 の通信装置に送信し、

前記第 2 の通信装置において、受信した前記要求に応じた所定の処理を行い、

前記第 2 の通信装置において、前記要求に含まれる前記個人識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、

前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第 1 の通信装置の前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第 1 の通信装置によるものであるかを判断する

通信方法。

【請求項 9 9】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第 1 の通信装置の前記装置識別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う  
請求項 9 8 に記載の通信方法。

【請求項 1 0 0】

前記通信制御装置は、

前記応答に含まれる前記装置識別情報と予め保持した前記第 1 の通信装置の前記装置識別情報とが一致しない場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う

請求項 9 8 に記載の通信方法。

【請求項 1 0 1】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

情報記録方法。

【請求項 1 0 2】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 1 0 1 に記載の情報記録方法。

【請求項 1 0 3】

前記所定の情報を暗号化し、

当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する

請求項 1 0 1 に記載の情報記録方法。

【請求項 1 0 4】

前記複数のモジュールをそれぞれ暗号化し、

当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する

請求項 1 0 1 に記載の情報記録方法。

【請求項 1 0 5】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、

当該読み出したモジュールを合成して前記所定の情報を復元する  
情報復元方法。

【請求項 1 0 6】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 1 0 5 に記載の情報復元方法。

【請求項 1 0 7】

前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する  
請求項 1 0 5 に記載の情報復元方法。

【請求項 1 0 8】

前記読み出したモジュールを復号した後に合成して前記所定の情報を復元する  
請求項 1 0 5 に記載の情報復元方法。

【請求項 1 0 9】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所  
定の情報を分割する情報分割手段と、

前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる  
領域に書き込む書き込み手段と

を有する情報記録装置。

【請求項 1 1 0】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に  
相互に独立している記録媒体である

請求項 1 0 9 に記載の情報記録装置。

【請求項 1 1 1】

前記所定の情報を暗号化する暗号化手段

をさらに有し、

前記情報分割手段は、

前記暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持  
される前記複数のモジュールに分割する

請求項 1 0 9 に記載の情報記録装置。

【請求項 1 1 2】

前記複数のモジュールをそれぞれ暗号化する暗号化手段

をさらに有し、

前記書き込み手段は、

前記暗号化によって得られた複数のモジュールを相互に異なる記録媒体または  
同一の記録媒体の異なる領域に書き込む

請求項 1 0 9 に記載の情報記録装置。

【請求項 1 1 3】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と、

当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段と

を有する情報復元装置。

【請求項 1 1 4】

前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である

請求項 1 1 3 に記載の情報復元装置。

【請求項 1 1 5】

前記合成して得た情報を復号する復号手段

をさらに有する

請求項 1 1 3 に記載の情報復元装置。

【請求項 1 1 6】

前記読み出したモジュールを復号する復号手段

をさらに有し、

前記情報合成手段は、前記復号したモジュールを合成して前記所定の情報を復元する

請求項 1 1 3 に記載の情報復元装置。

【請求項 1 1 7】

それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうち一のモジュールが記録された

記録媒体。

【発明の詳細な説明】

【0 0 0 1】

## 【発明の属する技術分野】

本発明は、他人の個人ＩＤ情報を不正に用いた手続を防止できる認証装置、認証システムおよびその方法、処理装置、通信装置、通信制御装置、通信システムおよびその方法、記録媒体に保持される情報の秘匿性を高めることができる情報記録方法およびその装置、情報復元方法およびその装置並びに記録媒体に関する。

## 【０００２】

## 【従来の技術】

インターネットなどのネットワークを介した電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行う受注者サーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人ＩＤ情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

## 【０００３】

また、近年、電子商取引の発達に伴い、ユーザの個人ＩＤ情報や暗証番号、取引の履歴情報、ユーザの名前、住所、経歴および職業などの個人情報などの秘匿性のある情報を、サーバ装置や端末装置などが管理するケースが多くなっている。

サーバ装置や端末装置では、例えば、特開平１１－２７２６７８１号公報に示されるように、上述したような秘匿性のある情報を、所定の暗号鍵で暗号化して、コンピュータに内蔵されたＨＤＤ（Hard Disk Drive）や、携帯性のあるＣＤ－ＲＯＭ、フロッピーディスク、ＰＣカードなどの記録媒体に記録している。

## 【０００４】

## 【発明が解決しようとする課題】

しかしながら、上述したネットワークを介した従来の電子商取引では、発注者および受注者の当事者間でのみ取り引きが行われることから、偽発注および商取引情報の改竄などの不正を取り締まりことが困難であるという問題がある。

また、このような電子商取引について第3者が認証を行う場合でも、他人の個人ID情報を用いてネットワークを介して行われる不正な手続（いわゆる、なりすまし）が行われる可能性があるという問題がある。

#### 【0005】

また、上述したような電子商取引が普及すると、複数の認証機関が、電子商取引の認証業務を行うことになる。この場合に、同じ電子商取引に参加した利用者が、それぞれ異なる認証機関と契約をしている場合に、どのようにして当該電子商取引の正当性を認証するかが課題となる。

この場合に、同じ電子商取引に参加した利用者が契約した複数の認証機関で、利用者の情報を共有することで、上述した課題に対処できるが、利用者の個人情報、他の機関に漏れてしまうという問題がある。

#### 【0006】

また、家庭内に複数の端末装置を設けた場合に、外部のネットワークを介して行われる電子商取引やセキュリティに関する機能を端末装置毎に持たせると、効率が悪いと共に、例えば家庭単位で通信履歴を管理するときに不便である。

#### 【0007】

また、上述した従来のサーバ装置や端末装置では、通常、秘匿性のある情報を単体の記録媒体に記録しており、その記録媒体が盗まれたり、不正にコピーされると、当該情報の秘匿性が失われてしまうという問題がある。

このような秘匿性のある情報は、通常、暗号化されて記録媒体に記録されるが、暗号化は復号（解読）される可能性があり、秘匿性を保持する上で十分ではない。

#### 【0008】

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人ID情報に基づいて不正な手続が行われることを回避する認証装置、認証システムおよびその方法を提供することを目的とする。

## 【0009】

また、本発明は、異なる認証機関と契約した利用者相互間の取り引きの認証を、利用者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供することを目的とする。

## 【0010】

また、本発明は、複数の端末装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供することを目的とする。

## 【0011】

また、本発明は、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法、情報復元方法およびそれらの装置と記録媒体を提供することを目的とする。

## 【0012】

## 【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の発明の認証装置は、ネットワークを介して少なくとも2者間で行われる取り引きを認証する認証装置であって、第1の取り引き者の個人識別情報、第2の取り引き者の個人識別情報および取り引き内容を示す情報を含む第1の要求を、前記第1の取り引き者から受信する第1の受信手段と、前記第1の要求に応じて、前記第1の取り引き者の正当性を認証して第1の認証情報を生成する第1の認証手段と、前記第1の認証情報および前記取り引きの内容を示す情報を含む第2の要求を前記第2の取り引き者に送信する第1の送信手段と、前記第2の要求に対しての応答を前記第2の取り引き者から受信する第2の受信手段と、前記応答に応じて、前記第2の取り引き者の正当性を認証して第2の認証情報を生成する第2の認証手段と、前記第2の認証情報を前記第1の取り引き者に送信する第2の送信手段とを有する。

## 【0013】

第1の発明の認証装置の作用は以下ようになる。

第 1 の受信手段によって、第 1 の取り引き者の個人識別情報、第 2 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求が、前記第 1 の取り引き者から受信される。

次に、第 1 の認証装置によって、前記第 1 の要求に応じて、前記第 1 の取り引き者の正当性が認証され、第 1 の認証情報が生成される。

次に、第 1 の送信手段によって、前記第 1 の認証情報および前記取り引きの内容を示す情報を含む第 2 の要求が前記第 2 の取り引き者に送信される。

そして、第 2 の受信手段によって、前記第 2 の要求に対しての応答が前記第 2 の取り引き者から受信される。

次に、第 2 の認証手段によって、前記応答に応じて、前記第 2 の取り引き者の正当性が認証され、第 2 の認証情報が生成される。

次に、第 2 の送信手段によって、前記第 2 の認証情報が前記第 1 の取り引き者に送信される。

#### 【 0 0 1 4 】

上述したように、第 1 の発明によれば、第 1 の取り引き者と第 2 の取り引き者とが通信を行って取り引きを行う場合に、第 1 の取り引き者および第 2 の取り引き者以外の第 3 者が管理する当該認証装置を用いることで、第 1 の取り引き者の正当性を客観的に認証した結果である第 1 の認証情報を第 2 の取り引き者に送信し、第 2 の取り引き者の正当性を客観的に認証した結果である第 2 の認証情報を第 1 の取り引き者に送信することができ、取り引きの信頼性を高めることが可能になる。

#### 【 0 0 1 5 】

第 1 の発明は、好ましくは、前記第 1 の受信手段は、前記第 1 の取り引き者の個人キー情報をさらに含む前記第 1 の要求を受信し、前記第 1 の認証手段は、前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証し、前記第 2 の受信手段は、前記第 2 の取り引き者の個人キー情報を含む前記応答を受信し、前記第 1 の認証手段は、前記第 2 の取り引き者の個人キー情報に基づいて前記第 2 の取り引き者の正当性を認証する。

ここで、前記第 1 の取り引き者および前記第 2 の取り引き者の前記個人キー情



報は、それぞれ前記第 1 の取り引き者および前記第 2 の取り引き者の課金に係わる情報である。

【 0 0 1 6 】

第 1 の発明の認証装置は、好ましくは、前記第 1 の送信手段は、前記第 1 の取り引き者の前記個人キー情報をさらに含む第 2 の要求を前記第 2 の取り引き者に送信する。

【 0 0 1 7 】

第 1 の発明の認証装置は、好ましくは、前記取り引きの履歴を示す履歴情報を記憶する記憶手段をさらに有する。

【 0 0 1 8 】

第 2 の発明の認証システムは、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証システムであって、第 1 の取り引き者が使用する第 1 の通信装置と、第 2 の取り引き者が使用する第 2 の通信装置と、前記取り引きを認証する認証装置とを有し、前記第 1 の通信装置は、第 1 の取り引き者の個人識別情報、第 2 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を前記認証装置に送信し、前記認証装置は、前記第 1 の取り引き者から前記第 1 の要求を受信する第 1 の受信手段と、前記第 1 の要求に応じて、前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、前記第 1 の認証情報および前記取り引きの内容を示す情報を含む第 2 の要求を前記第 2 の取り引き者に送信する第 1 の送信手段と、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段とを有する。

ここで、第 2 の発明の認証システムの前記認証装置の作用は前述した第 1 の発明の認証装置の作用と同じである。

【 0 0 1 9 】

第 3 の発明の認証方法は、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証方法であって、第 1 の取り引き者の個人識別情報、第 2

の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信し、前記第 1 の要求に応じて、前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成し、前記第 1 の認証情報および前記取り引きの内容を示す情報を含む第 2 の要求を前記第 2 の取り引き者に送信し、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信し、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成し、前記第 2 の認証情報を前記第 1 の取り引き者に送信する。

【 0 0 2 0 】

第 4 の発明の認証装置は、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証装置であって、第 1 の取り引き者の個人識別情報、前記第 1 の取り引き者の個人キー情報、第 2 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認証手段と、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信する第 1 の送信手段と、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、前記第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段とを有する。

【 0 0 2 1 】

第 4 の発明の認証装置の作用は以下になる。

第 1 の受信手段によって、第 1 の取り引き者の個人識別情報、第 2 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求が、前記第 1 の取り引き者から受信される。

次に、第 1 の認証装置によって、前記第 1 の要求に応じて、前記第 1 の取り引き者の正当性が認証され、第 1 の認証情報が生成される。

次に、第 1 の送信手段によって、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求が前記

第 2 の取り引き者に送信される。

そして、第 2 の受信手段によって、前記第 2 の要求に対しての応答が前記第 2 の取り引き者から受信される。

次に、第 2 の認証手段によって、前記応答に応じて、前記第 2 の取り引き者の正当性が認証され、第 2 の認証情報が生成される。

次に、第 2 の送信手段によって、前記第 2 の認証情報が前記第 1 の取り引き者に送信される。

#### 【 0 0 2 2 】

第 4 の発明の認証装置によれば、第 1 の送信手段から第 2 の取り引き者に送信される第 2 の要求には、前記第 1 の取り引き者の個人キー情報が含まれていないため、第 2 の取り引き者に、第 1 の取り引き者の課金に係わる情報が漏れることを回避できる。

#### 【 0 0 2 3 】

第 4 の発明の認証装置は、好ましくは、前記第 2 の受信手段は、前記第 2 の取り引き者の個人キー情報を含む前記応答を受信し、前記第 1 の認証手段は、前記第 2 の取り引き者の個人キー情報に基づいて前記第 2 の取り引き者の正当性を認証する。

ここで、前記第 1 の取り引き者の個人キー情報は前記第 1 の取り引き者の課金に係わる情報であり、前記第 2 の取り引き者の個人キー情報は前記第 2 の取り引き者の課金に係わる情報である。

#### 【 0 0 2 4 】

第 5 の発明の認証システムは、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証システムであって、第 1 の取り引き者が使用する第 1 の通信装置と、第 2 の取り引き者が使用する第 2 の通信装置と、前記取り引きを認証する認証装置とを有し、前記認証装置は、第 1 の取り引き者の個人識別情報、前記第 1 の取り引き者の個人キー情報、第 2 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信する第 1 の受信手段と、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成する第 1 の認

証手段と、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信する第 1 の送信手段と、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信する第 2 の受信手段と、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成する第 2 の認証手段と、前記取り引きの正当性を示す第 2 の認証情報を前記第 1 の取り引き者に送信する第 2 の送信手段とを有する。

## 【 0 0 2 5 】

第 5 の発明の認証システムの前記認証装置の作用は前述した第 4 の発明の認証装置の作用と同じである。

## 【 0 0 2 6 】

第 6 の発明の認証方法は、ネットワークを介して少なくとも 2 者間で行われる取り引きを認証する認証方法であって、第 1 の取り引き者の個人識別情報、前記第 1 の取り引き者の個人キー情報、第 2 の取り引き者の個人識別情報および取り引き内容を示す情報を含む第 1 の要求を、前記第 1 の取り引き者から受信し、前記第 1 の要求に含まれる前記個人キー情報に基づいて前記第 1 の取り引き者の正当性を認証して第 1 の認証情報を生成し、前記第 1 の要求から前記第 1 の取り引き者の個人キー情報を除去した情報と、前記第 1 の認証情報とを含む第 2 の要求を前記第 2 の取り引き者に送信し、前記第 2 の要求に対しての応答を前記第 2 の取り引き者から受信し、前記応答に応じて、前記第 2 の取り引き者の正当性を認証して第 2 の認証情報を生成し、前記第 2 の認証情報を前記第 1 の取り引き者に送信する。

## 【 0 0 2 7 】

第 7 の発明の認証装置は、認証要求に応じて認証処理を行う認証装置であって、利用者を識別するための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読

み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段とを有する。

## 【 0 0 2 8 】

第 7 の発明の認証装置の作用は以下ようになる。

例えば、利用者が端末装置などを操作して当該端末装置から送信された、利用者を識別するための個人識別情報と、認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求が受信手段で受信される。

次に、当該受信された前記認証要求に応じた認証処理が認証処理手段で行われる。

次に、送信手段によって、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とが対応付けて送信手段から送信される。

## 【 0 0 2 9 】

第 7 の発明の認識装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段をさらに有する。

また、第 7 の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する。

また、第 7 の発明の認証装置は、好ましくは、前記個人識別情報は、登録した利用者に予め割り当てられた識別子である。

また、第 7 の発明の認証装置は、好ましくは、前記装置識別情報は、前記装置の製造元で付された当該装置を一意に識別可能な識別子である。

## 【 0 0 3 0 】

第 8 の発明の認証装置は、ネットワークを介して行われる取引に関する認証処理を行う認証装置であって、利用者を識別するための個人識別情報と、取り

引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取り引きを行う利用者による前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記受信した認証要求に含まれる前記取り引き情報を前記認証要求によって指定された利用者の装置に送信し、当該指定された利用者の装置からの応答に応じて、所定の認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信する送信手段とを有する。

## 【 0 0 3 1 】

第 8 の発明の認証装置の作用は以下になる。

利用者を識別するための個人識別情報と、取り引きの内容を示す取り引き情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含み前記取り引きを行う利用者による前記認証要求が受信手段で受信される。

次に、認証処理手段によって、前記受信した認証要求に含まれる前記取り引き情報が前記認証要求によって指定された利用者の装置に送信され、当該指定された利用者の装置からの応答に応じて、所定の認証処理が行われる。

次に、送信手段によって、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記認証処理の結果と、前記認証要求に含まれる前記装置識別情報とを対応付けて送信手段から送信される。

## 【 0 0 3 2 】

第 8 の発明の認証装置は、好ましくは、前記認証処理手段は、前記取り引き情報に当該認証装置の認証結果を示す署名情報を付して前記指定された利用者の装置に送信し、前記指定された利用者からの応答に応じて、当該認証装置の署名情報を前記認証処理の結果として生成する。

## 【 0 0 3 3 】

第 8 の発明の認証装置は、好ましくは、前記記憶手段は、前記認証要求を発し

た利用者と前記指定された利用者との間の取り引きの履歴情報を記憶する。

【 0 0 3 4 】

第 8 の発明の認証装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報および前記装置識別情報を含む前記認証要求を受信し、前記認証装置は、前記受信した認証要求に含まれる前記個人識別情報および前記装置識別情報を復号する復号手段をさらに有する。

【 0 0 3 5 】

また、第 8 の発明の認証装置は、好ましくは、前記受信手段は、前記利用者に関する課金処理に用いられる第 3 の識別情報をさらに含む前記認証要求を受信する。

また、第 8 の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

【 0 0 3 6 】

第 9 の発明の処理装置は、ネットワークを介して行われる取り引きに関する認証要求を行う処理装置であって、利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む前記認証要求を送信する送信手段と、認証要求の送信元の装置を識別するための識別情報を含む認証応答を受信する受信手段と、前記装置識別情報と、前記認証応答に含まれる識別情報とが一致するか否かを判断する制御手段とを有する。

【 0 0 3 7 】

第 9 の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、所定の通知を前記認証応答の送信元に通知する。

また、第 9 の発明の処理装置は、好ましくは、前記制御手段は、前記認証応答に含まれる識別情報とが一致しないと判断した場合に、前記認証応答に含まれる当該認証の結果が用いられる取り引きの取り引き先の装置に所定の通知を行う。

【 0 0 3 8 】

第 1 0 の発明の認証システムは、ネットワークを介して接続される処理装置および認証装置を有する認証システムであって、前記認証装置は、利用者を識別す

るための個人識別情報と、前記認証要求の送信元の装置を識別する装置識別情報とを含む前記認証要求を受信する受信手段と、前記個人識別情報と認証結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記認証要求に応じて認証処理を行う認証処理手段と、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信する送信手段とを有し、前記処理装置は、前記個人識別情報と、当該処理装置を識別するための前記装置識別情報とを含む前記認証要求を送信する送信手段と、前記認証応答を受信する受信手段と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する制御手段とを有する。

## 【 0 0 3 9 】

第 1 1 の発明の認証方法は、ネットワークを介して接続される処理装置および認証装置を有する認証方法であって、利用者を識別するための個人識別情報と、当該処理装置を識別するための装置識別情報とを含む認証要求を前記処理装置から前記認証装置に送信し、前記認証装置において前記認証要求に応じて認証処理を行い、前記認証装置から、前記認証要求に含まれる前記個人識別情報に対応する前記送信先の情報によって特定された前記処理装置に、前記認証処理の結果と前記認証要求に含まれる前記装置識別情報とを含む認証応答を送信し、前記処理装置において、前記認証装置から受信した前記認証応答に含まれる前記装置識別情報と、当該処理装置の前記装置識別情報と、前記認証応答に含まれる前記装置識別情報とが一致するか否かを判断する。

## 【 0 0 4 0 】

第 1 2 の発明の認証装置は、第 1 の取り引き者に関する情報を保持し、第 2 の取り引き者に関する情報を保持する他の認証装置との間で通信を行いながらネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証装置であって、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を前



記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置による認証結果を示す第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から所定の応答を受ける送受信手段と、前記所定の応答を受けた場合に、前記取り引きの履歴を記憶する記憶手段と、前記所定の応答を受けた場合に、前記送受信手段を介して前記第 1 の取り引き者が使用する装置に送信される第 2 の署名情報であって、前記取り引きの正当性の認証結果を示す第 2 の署名情報を作成する署名作成手段とを有する。

## 【 0 0 4 1 】

第 1 2 の発明の認証装置の作用は以下のようになる。

送受信手段、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者からの第 1 の要求を受ける。

そして、当該第 2 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求が、前記送受信手段から前記第 2 の認証装置に送信される。

次に、送受信手段は、前記第 2 の要求に応じた第 1 の署名情報を前記第 2 の認証装置から受信する。

次に、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を、前記送受信手段から前記第 2 の取り引き者が使用する装置に送信する。

次に、送受信手段は、当該第 3 の要求に応じて前記第 2 の取り引き者が使用する装置から所定の応答を受ける。

前記送受信手段が前記所定の応答を受けると、記憶手段に、前記取り引きの履歴が記憶される。

また、前記送受信手段が前記所定の応答を受けると、署名作成手段によって、前記取り引きの正当性を認証する第 2 の署名情報が作成され、当該第 2 の署名情報が、前記送受信手段を介して前記第 1 の取り引き者が使用する装置に送信される。

## 【 0 0 4 2 】

第 1 2 の発明の認証装置は、好ましくは、暗号化手段をさらに有し、前記送受信手段は、前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記他の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取り引き者が使用する装置に送信する。

## 【 0 0 4 3 】

第 1 2 の発明の認証装置は、好ましくは、前記送受信手段は、前記他の認証装置が前記第 2 の取り引き者を識別するために用いる識別情報を含む前記所定の応答を前記第 2 の取り引き者が使用する装置から受け、前記記憶手段は、前記識別情報を用いて生成された前記取り引きの履歴を記憶する。

## 【 0 0 4 4 】

第 1 2 の発明の認証装置は、好ましくは、前記送受信手段は、前記第 1 の要求に含まれる前記取り引き内容に関する情報のうち、前記第 1 の取り引き者の課金に係わる情報以外の情報と、前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する。

## 【 0 0 4 5 】

第 1 2 の発明の認証装置は、好ましくは、前記送受信手段は、前記第 1 の要求に含まれる前記取り引き内容に関する情報と、前記第 1 の署名情報と、当該認証装置との間の通信に用いる暗号鍵とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信する。

## 【 0 0 4 6 】

第 1 2 の発明の認証装置は、好ましくは、前記取り引きに関する認証に対しての課金処理を行う課金処理手段をさらに有する。

## 【 0 0 4 7 】

第 1 2 の発明の認証装置は、好ましくは、前記課金処理手段は、前記他の認証装置との間で、前記取り引きに関する認証に対して行う課金の割合を決定するための処理を行う。

## 【 0 0 4 8 】

第 1 2 の発明の認証装置は、好ましくは、前記送受信手段は、前記第 2 の取り

引き者が前記第 1 の署名情報の正当性を確認して、当該取り引きに同意した場合に、前記第 2 の取り引き者が使用する装置から、前記記所定の応答を受ける。

## 【 0 0 4 9 】

第 1 3 の発明の認証システムは、ネットワークを介して少なくとも 2 者間で行われた取り引きを認証する認証システムであって、第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを有し、前記第 1 の認証装置は、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む前記第 1 の取り引き者による第 1 の要求に応じて、前記第 2 の取り引き者を特定する情報を含む第 2 の要求を前記第 2 の認証装置に送信し、前記第 2 の要求に応じた前記第 2 の認証装置からの第 1 の署名情報を受信し、前記第 1 の要求に含まれる前記取り引き内容に関する情報と前記第 1 の署名情報とを含む第 3 の要求を前記第 2 の取り引き者が使用する装置に送信し、当該第 3 の要求に応じて前記第 2 の取り引き者から所定の応答を受けると、前記取り引きの履歴を記憶し、前記取り引きの正当性を認証する第 2 の署名情報を前記第 1 の取り引き者に提供する。

## 【 0 0 5 0 】

第 1 3 の発明の認証システムは、前記第 1 の認証装置は、暗号化手段をさらに有し、前記送受信手段は、前記第 2 の取り引き者との間の通信に用いる暗号鍵を前記第 2 の要求に応じて前記第 2 の認証装置から受信し、前記暗号化手段で前記暗号鍵を用いて暗号化された前記取り引き内容に関する情報と前記第 1 の署名情報とを、前記第 2 の取り引き者が使用する装置に送信する。

## 【 0 0 5 1 】

第 1 4 の発明の認証方法は、第 1 の取り引き者に関する取り引きを認証する第 1 の認証装置と、第 2 の取り引き者に関する取り引きを認証する第 2 の認証装置とを用いて、ネットワークを介して行われる前記第 1 の取り引き者と前記第 2 の取り引き者との間の取り引きに関する認証を行う認証方法であって、前記第 1 の取り引き者から前記第 1 の認証装置に、前記取り引き内容を示す情報と前記第 2 の取り引き者を特定する情報とを含む第 1 の要求を出し、前記第 1 の要求に応じて、前記第 1 の認証装置から前記第 2 の認証装置に、前記第 2 の取り引き者を特

定する情報を含む第2の要求を送信し、前記第2の要求に応じて、前記第2の認証装置からの前記第1の認証装置に、当該第2の認証装置による認証結果を示す第1の署名情報を送信し、前記第1の認証装置から前記第2の取り引き者が使用する装置に、前記第1の要求に含まれる前記取り引き内容に関する情報と前記第1の署名情報とを含む第3の要求を送信し、当該第3の要求に応じて、前記第2の取り引き者が使用する装置から前記第1の認証装置に所定の応答を出し、前記所定の応答に応じて、前記第1の認証装置は、前記取り引きの履歴を記憶し、前記取り引きの正当性の認証結果を示す第2の署名情報を作成し、当該第2の署名情報を、前記第1の取り引き者が使用する装置に送信する。

## 【 0 0 5 2 】

第15の発明の通信装置は、利用者を識別するための個人識別情報を含む要求を受信する受信手段と、前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段とを有する。

## 【 0 0 5 3 】

第15の発明の通信装置の作用は以下になる。

例えば、利用者が他の通信装置を操作して、利用者を識別するための個人識別情報を含む要求を送信する。

当該要求は、受信手段で受信される。

次に、処理手段において、当該受信した要求に応じた所定の処理が行われる。

次に、送信手段によって、前記受信した要求に含まれる前記個人識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記処理の結果が送信される。

## 【 0 0 5 4 】

第15の発明の通信装置は、好ましくは、前記受信手段は、暗号化された前記個人識別情報を含む前記要求を受信し、前記通信装置は、前記受信した要求に含まれる前記個人識別情報を復号する復号手段をさらに有する。

また、第15の発明の通信装置は、好ましくは、前記個人識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である。

また、第15の発明の通信装置は、好ましくは、前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である。

また、第15の発明の通信装置は、好ましくは、前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための個人識別情報である。

また、第15の発明の通信装置は、好ましくは、前記処理は、認証処理である。

#### 【0055】

第16の発明の通信システムは、ネットワークを介して接続される第1の通信装置および第2の通信装置を有する通信システムであって、前記第1の通信装置は、利用者を識別するための個人識別情報を含む要求を受信する第1の受信手段と、前記個人識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第1の送信手段とを有し、前記第2の通信装置は、前記要求を前記第1の通信装置に送信する第2の送信手段と、前記処理の結果を前記第1の通信装置から受信する第2の受信手段と、当該受信した認証処理の結果を出力する出力手段とを有する。

#### 【0056】

第17の発明の通信方法は、ネットワークを介して接続される第1の通信装置および第2の通信装置を用いた通信方法であって、利用者を識別するための個人識別情報を含む要求を、前記第2の通信装置から前記第1の通信装置に送信し、前記第1の通信装置において、前記要求に応じて所定の処理を行い、前記第1の通信装置は、予め用意された前記個人識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記個人識別情報に対応する送

信先の情報によって特定される送信先に、前記処理の結果を送信する。

【 0 0 5 7 】

第 1 8 の発明の通信制御装置は、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関しての通信を制御する通信制御装置であって、前記第 1 の通信装置を識別するための装置識別情報を記憶する記憶手段と、前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報を含む要求を前記第 2 の通信装置に送信する送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する受信手段と、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段とを有する。

【 0 0 5 8 】

第 1 8 の発明の通信制御装置の作用は以下のようになる。

送信手段、第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報を含む要求を第 2 の通信装置に送信する。

そして、受信手段が、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する。

次に、制御手段によって、前記受信した応答に含まれる前記装置識別情報と記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する。

【 0 0 5 9 】

第 1 8 の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しない場合に、前記第 2 の通信装置に所定の通知を行う。

第 1 8 の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる装置識別情報と前記記憶手段に記憶された前記装置識別情報とが一致しな

い場合に、前記応答に含まれる処理の結果が用いられる取り引き先の装置に所定の通知を行う。

また、第 1 8 の発明の通信制御装置は、好ましくは、前記送信手段は、前記第 1 の通信装置から受信した個人識別情報と、当該第 1 の通信装置に対応する前記装置識別情報とを含む前記要求を前記第 2 の通信装置に送信する。

また、第 1 8 の発明の通信制御装置は、好ましくは、前記記憶手段は、前記第 1 の通信装置から受信した前記装置識別情報を記憶する。

【 0 0 6 0 】

また、第 1 8 の発明の通信制御装置は、好ましくは、前記記憶手段は、当該通信制御装置の電源が投入されたときに前記第 1 の通信装置から受信した前記装置識別情報を記憶する。

また、第 1 8 の発明の通信制御装置は、好ましくは、前記制御手段は、前記第 1 の通信装置と前記第 2 の通信装置との間の通信履歴を前記記憶手段に書き込む

また、第 1 8 の発明の通信制御装置は、好ましくは、前記制御手段は、前記応答に含まれる前記第 2 の通信装置の処理結果を、前記要求の送信元の前記第 1 の通信装置に送信する。

また、第 1 8 の発明の通信制御装置は、好ましくは、前記制御手段は、前記受信手段から受信した情報に応じて、待機状態にある前記第 1 の通信装置が動作状態になるように制御する。

また、第 1 8 の発明の通信制御装置は、好ましくは、前記制御手段は、前記第 1 の通信装置が接続されたネットワークと、前記第 2 の通信装置が接続されたネットワークとの間の通信を制御する。

また、第 1 8 の発明の通信制御装置は、好ましくは、前記装置識別情報は、前記第 1 の通信装置の製造元で付された当該通信装置を一意に識別可能な識別子である。

また、第 1 8 の発明の通信制御装置は、好ましくは、前記個人識別情報は、登録した利用者に予め割り当てられた識別子である。

【 0 0 6 1 】

第 1 9 の発明の通信システムは、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信システムであって、前記通信制御装置は、前記第 1 の通信装置を識別するための装置識別情報を記憶する第 1 の記憶手段と、前記第 1 の通信装置からの要求に応じて、当該第 1 の通信装置に対応する前記装置識別情報と個人識別情報とを含む要求を前記第 2 の通信装置に送信する第 1 の送信手段と、前記要求の送信元の装置を識別するための装置識別情報を含む応答を前記第 2 の通信装置から受信する第 1 の受信手段と、前記応答に含まれる前記装置識別情報と前記第 1 の記憶手段に記憶された前記装置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、前記第 1 の記憶手段に前記装置識別情報が記憶されている正当な前記第 1 の通信装置によるものであるかを判断する制御手段とを有し、前記第 2 の通信装置は、前記要求を受信する第 2 の受信手段と、前記個人識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する第 2 の記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記個人識別情報に対応する前記送信先の情報を前記第 2 の記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果と前記要求に含まれる前記装置識別情報とを対応付けて送信する第 2 の送信手段とを有する。

## 【 0 0 6 2 】

第 2 0 の発明の通信方法は、単数または複数の第 1 の通信装置からの要求に応じてネットワーク上の第 2 の通信装置で処理を行うことに関する通信を通信制御装置で制御する通信方法であって、前記第 1 の通信装置から前記通信制御装置に出された要求に応じて、当該第 1 の通信装置に対応する装置識別情報と個人識別情報とを含む要求を前記通信制御装置から前記第 2 の通信装置に送信し、前記第 2 の通信装置において、受信した前記要求に応じた所定の処理を行い、前記第 2 の通信装置において、前記要求に含まれる前記個人識別情報に対応する送信先の情報に基づいて、前記処理の結果と前記要求に含まれる前記装置識別情報とを含む応答を前記通信制御装置に送信し、前記通信制御装置において、受信した前記応答に含まれる前記装置識別情報と、予め保持した前記第 1 の通信装置の前記装



置識別情報とが一致するか否かに基づいて、前記受信した応答に対応した前記要求が、正当な前記第 1 の通信装置によるものであるかを判断する。

【 0 0 6 3 】

第 2 1 の発明の情報記録方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割し、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【 0 0 6 4 】

第 2 1 の発明の情報記録方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

また、第 2 1 の発明の情報記録方法は、好ましくは、前記所定の情報を暗号化し、当該暗号化によって得た情報を、それぞれ単独では所定の情報の秘匿性が保持される前記複数のモジュールに分割する。

また、第 2 1 の発明の情報記録方法は、好ましくは、前記複数のモジュールをそれぞれ暗号化し、当該暗号化によって得られた複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に記録する。

【 0 0 6 5 】

第 2 2 の発明の情報復元方法は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出し、当該読み出したモジュールを合成して前記所定の情報を復元する。

【 0 0 6 6 】

第 2 2 の発明の情報復元方法は、好ましくは、前記複数のモジュールが記録される相互に異なる複数の記録媒体は、物理的に相互に独立している記録媒体である。

また、第 2 2 の発明の情報復元方法は、好ましくは、前記読み出したモジュールを合成した後に復号して前記所定の情報を復元する。

また、第 2 2 の発明の情報復元方法は、好ましくは、前記読み出したモジュール

ルを復号した後に合成して前記所定の情報を復元する。

【0067】

第23の発明の情報記録装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割する情報分割手段と、前記複数のモジュールを相互に異なる記録媒体または同一の記録媒体の異なる領域に書き込む書き込み手段とを有する。

【0068】

第24の発明の情報復元装置は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールが相互に異なる複数の記録媒体または同一の記録媒体の異なる領域に記録されている場合に、前記複数の記録媒体または同一の記録媒体の異なる領域からそれぞれ前記モジュールを読み出す読み出し手段と当該読み出したモジュールを合成して前記所定の情報を復元する情報合成手段とを有する。

【0069】

第25の発明の記録媒体は、それぞれ単独では所定の情報の秘匿性が保持される複数のモジュールに前記所定の情報を分割した場合に、前記複数のモジュールのうちのモジュールが記録されている。

【0070】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムを図面を参照して説明する。

第1実施形態

図1は、本実施形態におけるトランザクション認証システム101の構成を示した構成図である。

トランザクション認証システム101は、発注者31が発注処理を行う発注者端末装置111と、発注者31の生体的特徴を利用して発注者31が本人であることを認証する生体認証装置12と、ネットワーク銀行（あるいはトランザクション認証局運営会社）121によって使用され、商取引情報の認証を行う認証装置113と、認証履歴を格納する認証履歴格納装置14と、受注者33が受注処理を行う受注者端末装置115とを有する。

本実施形態は、第４～７の発明に対応した実施形態であり、発注者端末装置１１１が本発明の第１の通信装置に対応し、認証装置１１３が本発明の認証装置に対応し、受注者端末装置１１５が本発明の第２の通信装置に対応している。また、発注者３１が本発明の第１の取り引き者に対応し、受注者３３が本発明の第２の取り引き者に対応している。

#### 【００７１】

##### 〔発注者端末装置１１１〕

図２は、発注者端末装置１１１の機能ブロック図である。

発注者端末装置１１１は、本システム利用の契約を行った一般利用者である発注者３１が使用する端末装置である。

発注者端末装置１１１は、図２に示すように、認証要求入力部１１１ａ、認証要求送信部１１１ｂ、認証応答受信部１１１ｃ、認証要求暗号化部１１１ｄおよび認証応答復号部１１１ｅを有する。

認証要求入力部１１１ａは、例えば、発注者３１によるキーボードなどの操作に応じて、発注情報ａ１および発注者個人キー情報ｋ１（本発明の第１の取り引き者の個人キー情報）の入力を行う。なお、本実施形態において、個人キー情報は、対応する者の課金に係わる情報である。

発注情報ａ１には、例えば、発注者３１の名前、住所、連絡先、受注者３３の個人ＩＤ情報ＩＤ２（本発明の第２の取り引き者の個人識別情報）および発注する商品またはサービスの内容が記述されている。

認証要求送信部１１１ｂは、認証要求入力部１１１ａに入力された発注情報ａ１および発注者個人キー情報を含む認証要求Ｉｎｆ１（本発明の第１の要求）を認証装置１１３に送信する。

認証応答受信部１１１ｃは、認証装置１１３から認証応答Ｉｎｆ４を受信する。

認証要求暗号化部１１１ｄは、認証要求Ｉｎｆ１を暗号化する。

認証応答復号部１１１ｅは、認証応答Ｉｎｆ４を復号する。

#### 【００７２】

生体認証装置１２は、いわゆるバイオメトリックス (biometrics) を用いて利

用者の個人認証を行う装置であり、具体的には、事前を取得し、生体認証装置 1 2 に格納しておいた利用者（発注者 3 1）の指紋等の身体的特徴と、実際に認証を行おうとする利用者の指紋等とを比較し、その一致・不一致によって本人の認証を行う。なお、利用者本人の指紋等の情報を格納する生体認証装置 1 2 の記録装置は、外部から電氣的に切断されており、その情報が外部に流出しない構成となっている。

## 【 0 0 7 3 】

## 〔認証装置 1 1 3〕

図 3 は、認証装置 1 1 3 の機能ブロック図である。

認証装置 1 1 3 は、本システムを運営するネットワーク銀行 1 2 1 が使用する装置である。

認証装置 1 1 3 は、図 3 に示すように、認証要求受信部 1 1 3 a、発注者認証部 1 1 3 b、要求生成部 1 1 3 c、要求送信部 1 1 3 d、応答受信部 1 1 3 e、受注者認証部 1 1 3 f、認証応答生成部 1 1 3 g、認証応答暗号化部 1 1 3 h、認証応答送信部 1 1 3 i、要求暗号化部 1 1 3 j、応答復号部 1 1 3 k および認証要求復号部 1 1 3 l を有する。

## 【 0 0 7 4 】

ここで、認証要求受信部 1 1 3 a が本発明の第 1 の受信手段に対応し、発注者認証部 1 1 3 b および要求生成部 1 1 3 c が本発明の第 1 の認証手段に対応し、要求送信部 1 1 3 d が本発明の第 1 の送信手段に対応し、応答受信部 1 1 3 e が本発明の第 2 の受信手段に対応し、受注者認証部 1 1 3 f および認証応答生成部 1 1 3 g が本発明の第 2 の認証手段に対応し、認証応答暗号化部 1 1 3 h が本発明の暗号化手段に対応し、認証応答送信部 1 1 3 i が本発明の第 2 の送信手段に対応し、要求暗号化部 1 1 3 j が本発明の暗号化手段に対応し、応答復号部 1 1 3 k が本発明の復号手段に対応し、認証要求復号部 1 1 3 l が本発明の復号手段に対応している。

## 【 0 0 7 5 】

認証要求受信部 1 1 3 a は、発注者端末装置 1 1 1 が送信した認証要求 I n f 1 を受信する。

発注者認証部 1 1 3 b は、認証要求 I n f 1 が含む発注者個人キー情報 k 1 を用いて発注者 3 1 の認証を行い、認証情報 A u 1（本発明の第 1 の認証情報）を生成する。

要求生成部 1 1 3 c は、認証要求 I n f 1 から個人キー情報 k 1 を削除して情報 I n f 1 a を生成し、当該情報 I n f 1 a と認証情報 A u 1 とを含む要求 I n f 2（本発明の第 2 の要求）を生成する。

要求送信部 1 1 3 d は、要求 I n f 2 を受注者端末装置 1 1 5 に送信する。

応答受信部 1 1 3 e は、受注者端末装置 1 1 5 から応答 I n f 3（本発明の応答）を受信する。

受注者認証部 1 1 3 f は、応答 I n f 3 に含まれる受注者 3 3 の個人 I D 情報 I D 2 および個人キー情報 k 2 を用いて受注者 3 3 の認証を行い、認証情報 A u 2（本発明の第 2 の識別情報）を生成する。

#### 【 0 0 7 6 】

認証応答生成部 1 1 3 g は、応答 I n f 3 に認証情報 A u 2 を付加して認証応答 I n f 4 を生成する。

認証応答暗号化部 1 1 3 h は、認証応答 I n f 4 を暗号化する。

認証応答送信部 1 1 3 i は、暗号化された認証応答 I n f 4 を発注者端末装置 1 1 1 に送信する。

要求暗号化部 1 1 3 j は、要求生成部 1 1 3 c が生成した要求 I n f 2 を暗号化する。

応答復号部 1 1 3 k は、応答 I n f 3 を復号する。

認証要求復号部 1 1 3 l は、認証要求 I n f 1 を復号する。

#### 【 0 0 7 7 】

##### 〔受注者端末装置 1 1 5〕

図 4 は、受注者端末装置 1 1 5 の機能ブロック図である。

受注者端末装置 1 1 5 は、本システム利用の契約を行った商品販売業者等である商品の受注者 3 3 が使用する。

受注者端末装置 1 1 5 は、要求受信部 1 1 5 a、要求復号部 1 1 5 b、応答入力部 1 1 5 c、応答生成部 1 1 5 d、応答暗号化部 1 1 5 e および応答送信部 1

15fを有する。

要求受信部115aは、認証装置113から要求Inf2を受信する。

要求復号部115bは、要求Inf2を復号する。

応答入力部115cは、ユーザによる操作に応じて、受注確認情報C1および受注者33の個人キー情報Zを入力する。

応答生成部115dは、要求Inf2、受注確認情報C1および受注者33の個人キー情報Zを含む応答Inf3を生成する。

応答暗号化部115eは、応答Inf3を暗号化する。

応答送信部115fは、暗号化された応答Inf3を認証装置113に送信する。

#### 【0078】

本実施形態のトランザクション認証システム101では、電子商取引の当事者である発注者31と受注者33との間に、その商取引の第三者であるネットワーク銀行121（あるいはトランザクション認証局）が介在し、ネットワーク銀行121が当事者間で行われる電子商取引を認証装置113を用いて認証することにより電子商取引上の不正を防止する。トランザクション認証システム101の利用を希望する商取引当事者は、まず、このネットワーク銀行121との間で認証装置13の利用契約を結ぶ。

#### 【0079】

例えば、図1に示すように、発注者31は、インターネット、郵便等を用い、ネットワーク銀行（トランザクション認証局運営会社）21に対して、契約に必要な情報の送付を行う。ここで送付する情報としては、発注者31の氏名、住所等の他、代金等の落とし先となる発注者31が契約している引き落とし銀行42の銀行口座等があげられる。これらの情報を受け取ったネットワーク銀行121は、契約を行った発注者31に対し、銀行42からの代金引き落としの際にその正当性を証明する個人ID情報、および本システムにおいて発注者31を識別するための個人キー情報の発行を行う。ここで発行された個人ID情報は銀行42に対しても送られ、銀行42は、商品等の代金引き落としの際にこの個人ID情報を認証し、代金の不正引き落としを防止する。

## 【0080】

なお、図1では、発注者31が利用契約を結ぶ場合についてのみ説明したが、商品販売業者等である商品の受注者33も同様な手順によりネットワーク銀行121との利用契約を結ぶ。また、ここでは、個人ID情報と個人キー情報を別個に発行することとしたが、個人キー情報を個人ID情報としても利用できることとし、別個の個人ID情報を発行しない形態としてもよい。

## 【0081】

次に、トランザクション認証システム101の動作について説明する。

ステップST11:

電子商取引によって商品を購入しようとする発注者31は、まず、インターネットの商取引サイト等から商品に関する情報を入手し、購入を希望する商品の選択を行う。

購入する商品の選択を行った発注者31は、次に、発注者31が所有する図2に示す発注者端末装置111を用いて、選択した商品の発注処理を行う。

発注処理は、認証要求入力部111aを用い、購入を希望する商品・数量等を指定する発注情報a1および発注者31の個人キー情報である発注者個人キー情報k1を入力することにより行う。ここで、発注者個人キー情報k1の入力は、発注処理を行うたびに発注者31が手動で行うこととしてもよいし、発注処理時、自動的に入力されることとしてもよい。

## 【0082】

これにより、入力された発注情報a1および発注者個人キー情報k1を含む認証要求Inf1が生成され、当該認証要求Inf1が認証要求暗号化部111dで暗号化された後、認証要求送信部111bを介して認証装置113に送信される。

このとき、認証要求送信部111bは、第三者による不正発注、児童のいたずら等による誤発注を防止するため、認証要求Inf1の送信を禁止する不正送信防止機能を有しており、この状態では認証要求Inf1の送信は行われない。

そのため、電子商取引を行おうとする発注者31は、生体認証装置12を用い、自己の認証を行い、この不正送信防止機能の解除を行う必要がある。

例えば、生体認証装置 12 が発注者 31 の指紋によって発注者 31 を認証するものであった場合、発注者 31 は、生体認証装置 12 に自己の指紋を読み取らせ、発注者 31 の指紋を読み取った生体認証装置 12 は、読み取った指紋と、事前取得し、内部に格納しておいた発注者 31 本人の指紋データとを照合し、読み取った指紋が発注者 31 本人のものであるか否かを判断する。

そして、読み取った指紋が発注者 31 本人のものであると判断された場合、生体認証装置 12 は、認証が成立した旨の情報を認証要求送信部 111b に指示を与え、この情報を受けた認証要求送信部 111b は、不正送信防止機能を解除し、送られた認証要求をトランザクション認証局 32 所有の認証装置 113 に送信する。

#### 【0083】

##### ステップ ST12 :

図 3 に示す認証装置 113 に送信された認証要求 Inf1 は、認証要求受信部 113a で受信され、認証要求復号部 113l によって復号された後、発注者認証部 113b に送られる。

次に、発注者認証部 113b において、認証要求 Inf1 に含まれる発注者個人キー情報 k1 と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な発注者 31 であるか否かが判断される。

そして、正当な発注者 31 であると判断されると、認証要求 Inf1 は要求生成部 113c に送られて、要求生成部 113c において、認証要求 Inf1 から個人キー情報 k1 を削除して生成された情報 Inf1a と、認証情報 Au1 とを含む要求 Inf2 (本発明の第 2 の要求) が生成される。

当該 Inf2 は、要求暗号化部 113j において暗号化された後に、要求送信部 113d を介して受注者端末装置 115 に送信される。

また、認証要求 Inf1 は、認証履歴格納装置 14 に認証履歴として記憶される。

#### 【0084】

##### ステップ ST13 :

受注者端末装置 115 に送信された要求 Inf2 は、要求受信部 115a によ



って受信された後、要求復号部 1 1 5 b により復号され、受注者 3 3 は、復号された要求 I n f 2 に基づいて商品の受注処理を行う。

受注処理は、受注者 3 3 が応答入力部 1 1 5 c を用い、受注確認情報 C 1 および受注者 3 3 の個人キー情報 Z（本発明の第 2 の取り引き者の個人キー情報）を入力することにより行われる。ここで、受注者個人キー情報 Z の入力、受注処理を行うたびに受注者 3 3 が手動で行うこととしてもよいし、発送処理時、自動的に入力されることとしてもよい。

#### 【 0 0 8 5 】

次に、応答生成部 1 1 5 d において、要求 I n f 2、受注確認情報 C 1 および受注者 3 3 の個人キー情報 Z を含む応答 I n f 3 が生成され、当該応答 I n f 3 が、応答暗号化部 1 1 5 e で暗号化された後に、応答送信部 1 1 5 f を介して認証装置 1 1 3 に送信される。

#### 【 0 0 8 6 】

ステップ S T 1 4 :

認証装置 1 1 3 に送信された応答 I n f 3 は、図 3 に示す応答受信部 1 1 3 e で受信され、応答復号部 1 1 3 k によって復号された後、受注者認証部 1 1 3 f に送られる。

次に、受注者認証部 1 1 3 f において、応答 I n f 3 に含まれる受注者個人キー情報 Z と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な受注者 3 3 であるか否かが判断される。

そして、正当な受注者 3 3 であると判断されると、応答 I n f 3 は認証応答生成部 1 1 3 g に送られて、認証応答生成部 1 1 3 g において、応答 I n f 3 と、認証が成立したことを示す認証情報 A u 2 とを含む認証応答 I n f 4 が生成される。

当該認証応答 I n f 4 は、認証応答暗号化部 1 1 3 h において暗号化された後に、認証応答送信部 1 1 3 i を介して発注者端末装置 1 1 1 に送信される。

また、応答 I n f 3 は、認証履歴格納装置 1 4 に認証履歴として記憶される。

#### 【 0 0 8 7 】

発注者端末装置 1 1 1 に送信された認証応答 I n f 4 は、図 2 に示す認証応答

受信部 111c で受信された後、認証応答復号手投 11e によって復号され、発注者 31 は、この復号された認証応答 Inf 4 を確認することにより、自己の商品発注が適正に受領された旨を知ることが可能となる。

その後、ネットワーク銀行 21 は、発注者 31 の個人キー情報 k1 を用いて、発注者 31 が契約する引き落とし銀行 42 の銀行口座から、当該取り引きに伴う金額を引き落とす。当該引き落としは、ネットワーク銀行 21 の銀行口座に引き落としてから受注者 33 の銀行口座に振り込んでもよいし、発注者 31 の銀行口座から受注者 33 の銀行口座に振り込みを直接行ってもよい。

また、受注者 33 は、発注情報 a1 に基づいて、発注者 31 に商品およびサービスを提供する。

#### 【0088】

以上説明したように、トランザクション認証システム 101 によれば、発注者端末装置 111 および受注者端末装置 115 を用いた、発注者 31 と受注者 33 との間の電子商取引を認証装置 113 を用いて認証することで、電子商取引の信頼性を高めることができる。

また、トランザクション認証システム 101 によれば、認証装置 113 から受注者端末装置 115 に送信される要求 Inf 2 には、受注者 33 の個人キー情報 k1 を含まないため、発注者 31 の課金に係わる個人キー情報が受注者 33 に渡ることはない。そのため、個人キー情報の不正利用を効果的に抑制できる。

また、トランザクション認証システム 101 によれば、第三者が発注者個人キー情報 k1 を盗用して偽発注を行った場合或いは情報の改竄を行った場合であっても、その発注に対する認証応答 Inf 4 は正規の発注者 31 に送信されることとなり、正規の発注者 31 は、第三者による偽発注或いは改竄があったことを知ることができ、これにより電子取引上の不正を有効に防止することが可能となる。

#### 【0089】

また、認証装置 113 によって、認証要求 Inf 1 および応答 Inf 3 を認証することとしたため、電子商取引においてやりとりされる情報の信頼性が増し、電子取引上の不正を有効に防止することが可能となる。

## 【0090】

さらに、認証履歴格納装置14によって、認証要求Inf1および応答Inf3を格納することとしたため、電子商取引の履歴を第三者が客観的に証明することが可能となり、これにより電子商取引の当事者間で行われる不正を有効に防止することが可能となる。

## 【0091】

また、認証要求Inf1、要求Inf2、応答Inf3および認証応答Inf4は、暗号化されて送信されることとしたため、第三者による情報の改竄、盗用等を有効に防止することが可能となる。

## 【0092】

さらに、認証要求送信部111bは、生体認証装置12によって発注者31が本人であることが認証された場合にのみ、認証要求の送信を行うこととしたため、第三者による不正発注、児童のいたずら等による誤発注を防止することが可能となる。

## 【0093】

## 第2実施形態

図6は、本実施形態におけるトランザクション認証システム1の構成を示した構成図である。

トランザクション認証システム1は、発注者31が発注処理を行う発注者端末装置11と、発注者31の生体的特徴を利用して発注者31が本人であることを認証する生体認証装置12と、ネットワーク銀行（あるいはトランザクション認証局運営会社）21によって使用され、商取引情報の認証を行う認証装置13と、認証履歴を格納する認証履歴格納装置14と、受注者33が受注処理を行う受注者端末装置15とを有する。

本実施形態は、第1～3の発明に対応した実施形態であり、発注者端末装置11が本発明の第1の通信装置に対応し、認証装置13が本発明の認証装置に対応し、受注者端末装置15が本発明の第2の通信装置に対応している。また、発注者31が本発明の第1の取り引き者に対応し、受注者33が本発明の第2の取り引き者に対応している。

## 【 0 0 9 4 】

## 〔発注者端末装置 1 1〕

図 7 は、発注者端末装置 1 1 の機能ブロック図である。

発注者端末装置 1 1 は、本システム利用の契約を行った一般利用者である発注者 3 1 が使用する端末装置である。

発注者端末装置 1 1 は、図 7 に示すように、認証要求入力部 1 1 a、認証要求送信部 1 1 b、認証応答受信部 1 1 c、認証要求暗号化部 1 1 d および認証応答復号部 1 1 e を有する。

認証要求入力部 1 1 a は、例えば、発注者 3 1 によるキーボードなどの操作に応じて、発注情報 a 1、発注者個人 ID 情報 ID 1（本発明の第 1 の取り引き者の個人識別情報）および発注者個人キー情報 k 1（本発明の第 1 の取り引き者の個人キー情報）の入力を行う。なお、本実施形態において、個人キー情報は、対応する者の課金に係わる情報である。

発注情報 a 1 には、例えば、発注者 3 1 の名前、住所、連絡先、受注者 3 3 の個人 ID 情報 ID 2（本発明の第 2 の取り引き者の個人識別情報）および発注する商品またはサービスの内容が記述されている。

認証要求送信部 1 1 b は、認証要求入力部 1 1 a に入力された発注情報 a 1、発注者個人 ID 情報 ID 1 および発注者個人キー情報を含む認証要求 Inf 1（本発明の第 1 の要求）を認証装置 1 3 に送信する。

認証応答受信部 1 1 c は、認証装置 1 3 から認証応答 Inf 4 を受信する。

認証要求暗号化部 1 1 d は、認証要求 Inf 1 を暗号化する。

認証応答復号部 1 1 e は、認証応答 Inf 4 を復号する。

## 【 0 0 9 5 】

生体認証装置 1 2 は、いわゆるバイオメトリックス (biometrics) を用いて利用者の個人認証を行う装置であり、具体的には、事前に取得し、生体認証装置 1 2 に格納しておいた利用者（発注者 3 1）の指紋等の身体的特徴と、実際に認証を行おうとする利用者の指紋等とを比較し、その一致・不一致によって本人の認証を行う。なお、利用者本人の指紋等の情報を格納する生体認証装置 1 2 の記録装置は、外部から電氣的に切断されており、その情報が外部に流出しない構成と

なっている。

【0096】

〔認証装置13〕

図8は、認証装置13の機能ブロック図である。

認証装置13は、本システムを運営するネットワーク銀行21が使用する装置である。

認証装置13は、図8に示すように、認証要求受信部13a、発注者認証部13b、要求生成部13c、要求送信部13d、応答受信部13e、受注者認証部13f、認証応答生成部13g、認証応答暗号化部13h、認証応答送信部13i、要求暗号化部13j、応答復号部13kおよび認証要求復号部13lを有する。

【0097】

ここで、認証要求受信部13aが本発明の第1の受信手段に対応し、発注者認証部13bおよび要求生成部13cが本発明の第1の認証手段に対応し、要求送信部13dが本発明の第1の送信手段に対応し、応答受信部13eが本発明の第2の受信手段に対応し、受注者認証部13fおよび認証応答生成部13gが本発明の第2の認証手段に対応し、認証応答暗号化部13hが本発明の暗号化手段に対応し、認証応答送信部13iが本発明の第2の送信手段に対応し、要求暗号化部13jが本発明の暗号化手段に対応し、応答復号部13kが本発明の復号手段に対応し、認証要求復号部13lが本発明の復号手段に対応している。

【0098】

認証要求受信部13aは、発注者端末装置11が送信した認証要求Inf1を受信する。

発注者認証部13bは、認証要求Inf1が含む発注者個人ID情報ID1および発注者個人キー情報k1を用いて発注者31の認証を行い、認証情報Au1（本発明の第1の認証情報）を生成する。

要求生成部13cは、発注者認証部13bによって認証された認証要求Inf1に認証情報Au1を付加して要求Inf2（本発明の第2の要求）を生成する。

要求送信部13dは、要求Inf2を受注者端末装置15に送信する。

応答受信部13eは、受注者端末装置15から応答Inf3（本発明の応答）を受信する。

受注者認証部13fは、応答Inf3に含まれる受注者33の個人ID情報ID2および個人キー情報k2を用いて受注者33の認証を行い、認証情報Au2（本発明の第2の識別情報）を生成する。

#### 【0099】

認証応答生成部13gは、応答Inf3に認証情報Au2を付加して認証応答Inf4を生成する。

認証応答暗号化部13hは、認証応答Inf4を暗号化する。

認証応答送信部13iは、暗号化された認証応答Inf4を発注者端末装置11に送信する。

要求暗号化部13jは、要求生成部13cが生成した要求Inf2を暗号化する。

応答復号部13kは、応答Inf3を復号する。

認証要求復号部13lは、認証要求Inf1を復号する。

#### 【0100】

##### 〔受注者端末装置15〕

図9は、受注者端末装置15の機能ブロック図である。

受注者端末装置15は、本システム利用の契約を行った商品販売業者等である商品の受注者33が使用する。

受注者端末装置15は、要求受信部15a、要求復号部15b、応答入力部15c、応答生成部15d、応答暗号化部15eおよび応答送信部15fを有する。

要求受信部15aは、認証装置13から要求Inf2を受信する。

要求復号部15bは、要求Inf2を復号する。

応答入力部15cは、ユーザによる操作に応じて、受注確認情報C1および受注者33の個人キー情報Zを入力する。

応答生成部15dは、要求Inf2、受注確認情報C1および受注者33の個

人キー情報Zを含む応答Inf3を生成する。

応答暗号化部15eは、応答Inf3を暗号化する。

応答送信部15fは、暗号化された応答Inf3を認証装置13に送信する。

#### 【0101】

本実施形態のトランザクション認証システム1では、電子商取引の当事者である発注者31と受注者33との間に、その商取引の第三者であるネットワーク銀行21（あるいはトランザクション認証局）が介在し、ネットワーク銀行21が当事者間で行われる電子商取引を認証装置13を用いて認証することにより電子商取引上の不正を防止する。トランザクション認証システム1の利用を希望する商取引当事者は、まず、このネットワーク銀行21との間で認証装置13の利用契約を結ぶ。

#### 【0102】

例えば、図6に示すように、発注者31は、インターネット、郵便等を用い、ネットワーク銀行21に対して、契約に必要な情報の送付を行う。ここで送付する情報としては、発注者31の氏名、住所等の他、代金等の落とし先となる発注者31が契約している引き落とし銀行42の銀行口座等があげられる。これらの情報を受け取ったネットワーク銀行21は、契約を行った発注者31に対し、銀行42からの代金引き落としの際にその正当性を証明する個人ID情報、および本システムにおいて発注者31を識別するための個人キー情報の発行を行う。ここで発行された個人ID情報は銀行42に対しても送られ、銀行42は、商品等の代金引き落としの際にこの個人ID情報を認証し、代金の不正引き落としを防止する。

#### 【0103】

なお、図6では、発注者31が利用契約を結ぶ場合についてのみ説明したが、商品販売業者等である商品の受注者33も同様な手順によりネットワーク銀行21との利用契約を結ぶ。また、ここでは、個人ID情報と個人キー情報を別個に発行することとしたが、個人キー情報を個人ID情報としても利用できることとし、別個の個人ID情報を発行しない形態としてもよい。

#### 【0104】

次に、トランザクション認証システム1の動作について説明する。

ステップST1:

電子商取引によって商品を購入しようとする発注者31は、まず、インターネットの商取引サイト等から商品に関する情報を入手し、購入を希望する商品の選択を行う。

購入する商品の選択を行った発注者31は、次に、発注者31が所有する図7に示す発注者端末装置11を用いて、選択した商品の発注処理を行う。

発注処理は、認証要求入力部11aを用い、購入を希望する商品・数量等を指定する発注情報a1、契約時に発行された発注者31の個人ID情報である発注者個人ID情報ID1、および発注者の個人キー情報である発注者個人キー情報k1を入力することにより行う。ここで、発注者個人ID情報ID1および発注者個人キー情報k1の入力は、発注処理を行うたびに発注者31が手動で行うこととしてもよいし、発注処理時、自動的に入力されることとしてもよい。

【0105】

これにより、入力された発注情報a1、発注者個人ID情報ID1および発注者個人キー情報k1を含む認証要求Inf1が生成され、当該認証要求Inf1が認証要求暗号化部11dで暗号化された後、認証要求送信部11bを介して認証装置13に送信される。

このとき、認証要求送信部11bは、第三者による不正発注、児童のいたずら等による誤発注を防止するため、認証要求Inf1の送信を禁止する不正送信防止機能を有しており、この状態では認証要求Inf1の送信は行われない。

そのため、電子商取引を行おうとする発注者31は、生体認証装置12を用い、自己の認証を行い、この不正送信防止機能の解除を行う必要がある。

例えば、生体認証装置12が発注者31の指紋によって発注者31を認証するものであった場合、発注者31は、生体認証装置12に自己の指紋を読み取らせ、発注者31の指紋を読み取った生体認証装置12は、読み取った指紋と、事前に取得し、内部に格納しておいた発注者31本人の指紋データとを照合し、読み取った指紋が発注者31本人のものであるか否か判断する。

そして、読み取った指紋が発注者31本人のものであると判断された場合、生



体認証装置 1 2 は、認証が成立した旨の情報を認証要求送信部 1 1 b に指示を与え、この情報を受けた認証要求送信部 1 1 b は、不正送信防止機能を解除し、送られた認証要求をネットワーク銀行 2 1 所有の認証装置 1 3 に送信する。

【 0 1 0 6 】

ステップ ST 2 :

図 8 に示す認証装置 1 3 に送信された認証要求 I n f 1 は、認証要求受信部 1 3 a で受信され、認証要求復号部 1 3 1 によって復号された後、発注者認証部 1 3 b に送られる。

次に、発注者認証部 1 3 b において、認証要求 I n f 1 に含まれる発注者個人 ID 情報 I D 1 と、発注者個人キー情報 k 1 と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な発注者 3 1 であるか否かが判断される。

そして、正当な発注者 3 1 であると判断されると、認証要求 I n f 1 は要求生成部 1 3 c に送られて、要求生成部 1 3 c において、認証要求 I n f 1 と、認証が成立したことを示す認証情報 A u 1 とを含む要求 I n f 2 が生成される。

当該 I n f 2 は、要求暗号化部 1 3 j において暗号化された後に、要求送信部 1 3 d を介して受注者端末装置 1 5 に送信される。

また、認証要求 I n f 1 は、認証履歴格納装置 1 4 に認証履歴として記憶される。

【 0 1 0 7 】

ステップ ST 3 :

受注者端末装置 1 5 に送信された要求 I n f 2 は、要求受信部 1 5 a によって受信された後、要求復号部 1 5 b により復号され、受注者 3 3 は、復号された要求 I n f 2 に基づいて商品の受注処理を行う。

受注処理は、受注者 3 3 が応答入力部 1 5 c を用い、受注確認情報 C 1 および受注者 3 3 の個人キー情報 Z (本発明の第 2 の取り引き者の個人キー情報)を入力することにより行われる。ここで、受注者個人キー情報 Z の入力、受注処理を行うたびに受注者 3 3 が手動で行うこととしてもよいし、発送処理時、自動的に入力されることとしてもよい。

## 【 0 1 0 8 】

次に、応答生成部 1 5 d において、要求 I n f 2、受注確認情報 C 1 および受注者 3 3 の個人キー情報 Z を含む応答 I n f 3 が生成され、当該応答 I n f 3 が、応答暗号化部 1 5 e で暗号化された後に、応答送信部 1 5 f を介して認証装置 1 3 に送信される。

## 【 0 1 0 9 】

ステップ S T 4 :

認証装置 1 3 に送信された応答 I n f 3 は、図 8 に示す応答受信部 1 3 e で受信され、応答復号部 1 3 k によって復号された後、受注者認証部 1 3 f に送られる。

次に、受注者認証部 1 3 f において、応答 I n f 3 に含まれる受注者個人キー情報 Z と、図示していない記録装置に格納された契約者の個人キー情報とを用いて正当な受注者 3 3 であるか否かが判断される。

そして、正当な受注者 3 3 であると判断されると、応答 I n f 3 は認証応答生成部 1 3 g に送られて、認証応答生成部 1 3 g において、応答 I n f 3 と、認証が成立したことを示す認証情報 A u 2 とを含む認証応答 I n f 4 が生成される。

当該認証応答 I n f 4 は、認証応答暗号化部 1 3 h において暗号化された後に、認証応答送信部 1 3 i を介して発注者端末装置 1 1 に送信される。

また、応答 I n f 3 は、認証履歴格納装置 1 4 に認証履歴として記憶される。

## 【 0 1 1 0 】

発注者端末装置 1 1 に送信された認証応答 I n f 4 は、図 7 に示す認証応答受信部 1 1 c で受信された後、認証応答復号手投 1 1 e によって復号され、発注者 3 1 は、この復号された認証応答 I n f 4 を確認することにより、自己の商品発注が適正に受領された旨を知ることが可能となる。その後、受注者 3 3 は、発注者 3 1 の発注者個人 I D 情報 I D 1 を用い、発注者 3 1 が契約している銀行から、発注を受けた商品代金の引き落としを行い、さらに、発注を受けた商品を発注者 3 1 に郵送する。

## 【 0 1 1 1 】

以上説明したように、トランザクション認証システム 1 によれば、発注者端末

装置 11 および受注者端末装置 15 を用いた、発注者 31 と受注者 33 との間の電子商取引を認証装置 13 を用いて認証することで、電子商取引の信頼性を高めることができる。

また、トランザクション認証システム 1 によれば、第三者が発注者個人キー情報 k1 を盗用して偽発注を行った場合或いは情報の改竄を行った場合であっても、その発注に対する認証応答 Inf 4 は正規の発注者 31 に送信されることとなり、正規の発注者 31 は、第三者による偽発注或いは改竄があったことを知ることができ、これにより電子取引上の不正を有効に防止することが可能となる。

#### 【0112】

また、認証装置 13 によって、認証要求 Inf 1 および応答 Inf 3 を認証することとしたため、電子商取引においてやりとりされる情報の信頼性が増し、電子取引上の不正を有効に防止することが可能となる。

#### 【0113】

さらに、認証履歴格納装置 14 によって、認証要求 Inf 1 および応答 Inf 3 を格納することとしたため、電子商取引の履歴を第三者が客観的に証明することが可能となり、これにより電子商取引の当事者間で行われる不正を有効に防止することが可能となる。

#### 【0114】

また、認証要求 Inf 1、要求 Inf 2、応答 Inf 3 および認証応答 Inf 4 は、暗号化されて送信されることとしたため、第三者による情報の改竄、盗用等を有効に防止することが可能となる。

#### 【0115】

さらに、認証要求送信部 11b は、生体認証装置 12 によって発注者 31 が本人であることが認証された場合にのみ、認証要求の送信を行うこととしたため、第三者による不正発注、児童のいたずら等による誤発注を防止することが可能となる。

#### 【0116】

なお、上記の処理機能は、コンピュータによって実現することができる。その場合、発注者端末装置 11、認証装置 13、受注者端末装置 15 が有すべき機能

の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述しておく。そして、このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場に流通させる場合には、CD-ROM (Compact Disc Read Only Memory) やフロッピーディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

## 【0117】

なお、本形態では、トランザクション認証システム1を、電子商取引において利用することとしたが、電子通信回線を用いたアンケート、投票、その他情報伝送時における不正防止のために利用することとしてもよい。

## 【0118】

第3実施形態

図11は、本実施形態のトランザクション認証システム301の全体構成図である。

図11に示すように、トランザクション認証システム301では、例えば、発注者31の発注者端末装置311と、受注者33の受注者端末装置315と、ネットワーク銀行340の認証装置350と、ネットワーク銀行341の認証装置351と、認証履歴を格納する認証履歴格納装置14とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者31と受注者33との間のトランザクション（取引）の正当性を認証する。

## 【0119】

本実施形態では、例えば、発注者31とネットワーク銀行340との間で認証を行うことについての契約が成されており、受注者33とネットワーク銀行341との間で認証を行うことについての契約が成されている。

また、ネットワーク銀行340とネットワーク銀行341とは、認証に関し

て、相互に連携する旨の相互乗り入れの契約が成立されている。

【0120】

本実施形態は、第12～14の発明に対応した実施形態である。

本実施形態では、発注者31が本発明の第1の取り引き者に対応し、受注者33が本発明の第2の取り引き者に対応している。

また、認証装置350が、第12の発明の認証装置、並びに第13の発明および第14の発明の第1の認証装置に対応している。

また、認証装置351が、第12の発明の他の認証装置、並びに第13の発明および第14の発明の第2の認証装置に対応している。

【0121】

以下、トランザクション認証システム301を構成する各装置について説明する。

〔発注者端末装置311〕

図12に示すように、発注者端末装置311は、例えば、発注者31の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部361、送信部362、暗号化部363、復号部364、記憶部365、制御部366および署名検証部367を有する。

なお、発注者端末装置311は、例えば、発注者31が使用する際に、発注者31の指紋等の身体的特徴から得られる情報と、予め記憶部365に予め記憶したある身体的特徴を示す情報とを比較することで、発注者31が正当な使用者であることを認証する生体認証部を有していてもよい。

【0122】

受信部361は、ネットワークを介して認証装置350から情報あるいは要求を受信する。

送信部362は、ネットワークを介して認証装置350に情報あるいは要求を送信する。

また、受信部361および送信部362は、受注者33が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 363 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 364 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 365 は、例えば、発注者 31 がネットワーク銀行 340 と契約を行うと、例えば、発注者 31 に割り当てられた秘密鍵  $K_{31,S}$  などを格納する。

制御部 366 は、発注者端末装置 311 内の各構成要素の処理を統括的に制御する。

署名検証部 367 は、例えば、認証装置 350 が作成した署名情報を、ネットワーク銀行 340 の公開鍵  $K_{40,P}$  を用いて検証する。

### 【0123】

#### 〔受注者端末装置 315〕

図 13 に示すように、受注者端末装置 315 は、サイバーモール (Cyber Mall) などに店舗を出している受注者 33 が使用するサーバ装置であり、受信部 371、送信部 372、暗号化部 373、復号部 374、記憶部 375、制御部 376 および署名検証部 377 を有する。

受信部 371 は、ネットワークを介して認証装置 350、351 から情報あるいは要求を受信する。

送信部 372 は、ネットワークを介して認証装置 350、351 に情報あるいは要求を送信する。

また、受信部 371 および送信部 372 は、発注者端末装置 311 からのアクセスに応じて、例えば、記憶部 375 から読み出した受注者 33 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 311 に送信する。

暗号化部 373 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 374 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 375 は、例えば、受注者 33 がネットワーク銀行 341 と契約を行うと、例えば、受注者 33 に割り当てられた秘密鍵  $K_{33,S}$  などを格納する。

制御部 376 は、受注者端末装置 315 内の各構成要素の処理を統括的に制御する。

署名検証部 377 は、例えば、受注者 33 の公開鍵  $K_{33,P}$  を用いて、受注者端末装置 315 が作成した署名情報の検証を行う。

## 【0124】

## 〔認証装置350〕

図14に示すように、認証装置350は、受信部381、送信部382、暗号化部383、復号部384、記憶部385、制御部386、署名作成部387および課金処理部388を有する。

ここで、受信部381および送信部382が、第12の発明の送受信手段に対応し、記憶部385が第12の発明の記憶手段に対応し、署名作成部387が第12の発明の署名作成手段に対応している。

## 【0125】

受信部381は、ネットワークを介して発注者端末装置311、受注者端末装置315および認証装置351から情報あるいは要求を受信する。

送信部382は、ネットワークを介して発注者端末装置311、受注者端末装置315および認証装置351に情報あるいは要求を送信する。

暗号化部383は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部384は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部385は、例えば、発注者31がネットワーク銀行340と契約を行うと、例えば、発注者31に割り当てられた秘密鍵 $K_{31,S}$ に対応する公開鍵 $K_{33,P}$ などを格納する。

制御部386は、認証装置350内の各構成要素の処理を統括的に制御する。

署名作成部387は、ネットワーク銀行340の秘密鍵 $K_{40,S}$ を用いて署名情報の作成を行う。

課金処理部388は、発注者31による取引に関する認証に対しての課金処理を行い、認証装置351との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

認証装置350の各構成要素の詳細な処理については、後述する動作例で記載する。

## 【0126】

図15に示すように、認証装置351は、受信部391、送信部392、暗号

化部 3 9 3、復号部 3 9 4、記憶部 3 9 5、制御部 3 9 6、署名作成部 3 9 7 および課金処理部 3 9 8 を有する。

受信部 3 9 1 は、ネットワークを介して受注者端末装置 3 1 5 および認証装置 3 5 0 から情報あるいは要求を受信する。

送信部 3 9 2 は、ネットワークを介して受注者端末装置 3 1 5 および認証装置 3 5 0 に情報あるいは要求を送信する。

暗号化部 3 9 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 3 9 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 3 9 5 は、受注者 3 3 がネットワーク銀行 3 4 1 と契約を行うと、例えば、受注者 3 3 に割り当てられた秘密鍵  $K_{33,S}$  に対応する公開鍵  $K_{33,P}$  などを格納する。

制御部 3 9 6 は、認証装置 3 5 1 内の各構成要素の処理を統括的に制御する。

署名作成部 3 9 7 は、ネットワーク銀行 3 4 1 の秘密鍵  $K_{41,S}$  を用いて署名情報の作成を行う。

課金処理部 3 9 8 は、受注者 3 3 による取引に関する認証に対しての課金処理を行い、認証装置 3 5 0 との間で、前記取引に関する認証に対して行う課金の割合を決定するための処理を行う。

#### 【 0 1 2 7 】

以下、トランザクション認証システム 3 0 1 の動作例を説明する。

以下に示す動作例を開始する前提として、発注者 3 1 とネットワーク銀行 3 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 3 4 0 は、発注者 3 1 に対して、個人キー情報  $k 1$  および個人 ID 情報  $ID 1$  を発行する。ネットワーク銀行 3 4 0 は、個人キー情報  $k 1$  および個人 ID 情報  $ID 1$  の対応表を図 1 4 に示す認証装置 3 5 0 の記憶部 3 8 5 に記憶する。ここで、個人キー情報  $k 1$  は、例えば、ネットワーク銀行 3 4 0 と契約した契約者（発注者 3 1）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報  $ID 1$  は、発注者 3 1 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、ネットワーク銀行 3 4 0 は、自らの秘密鍵  $K_{40,S}$  を図 1 4 に示す認証装置 3 5 0 の記憶部 3 8 5 に記憶すると共に、当該秘密鍵  $K_{40,S}$  に対応する公開鍵



$K_{40,P}$ を発注者端末装置 3 1 1 に送信する。発注者端末装置 3 1 1 は、公開鍵  $K_{40,P}$  を図 1 2 に示す記憶部 3 6 5 に記憶する。

#### 【0 1 2 8】

また、受注者 3 3 とネットワーク銀行 3 4 1 との間で所定の契約が結ばれ、ネットワーク銀行 3 4 1 は、受注者 3 3 に対して、個人キー情報  $Z$  および個人 ID 情報 ID 2 を発行する。ネットワーク銀行 3 4 1 は、個人キー情報  $Z$  および個人 ID 情報 ID 2 の対応表を図 1 5 に示す認証装置 3 5 1 の記憶部 3 9 5 に記憶する。

また、ネットワーク銀行 3 4 1 は、自らの秘密鍵  $K_{41,S}$  を図 1 5 に示す認証装置 3 5 1 の記憶部 3 9 5 に記憶すると共に、当該秘密鍵  $K_{41,S}$  に対応する公開鍵  $K_{41,P}$  を受注者端末装置 3 1 5 に送信する。受注者端末装置 3 1 5 は、公開鍵  $K_{41,P}$  を図 1 3 に示す記憶部 3 7 5 に記憶する。

#### 【0 1 2 9】

また、ネットワーク銀行 3 4 0 とネットワーク銀行 3 4 1 との間では、認証に関して相互乗り入れの契約がなされている。なお、認証装置 3 5 0 と認証装置 3 5 1 との間では、当該契約に基づいて、要求および情報の伝送が、公開鍵暗号方式あるいは共通鍵暗号方式を用いて行われる。

#### 【0 1 3 0】

図 1 6 は、トランザクション認証システム 3 0 1 の動作例を説明するための図である。

#### ステップ S T 3 1 :

発注者端末装置 3 1 1 は、図 1 1 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、受注者 3 3 を特定する情報（例えば受注者 3 3 の名前）、発注する商品名および数量などを示す発注情報  $a 1$  と、発注者 3 1 の個人キー情報  $k 1$  と、発注者 3 1 の個人 ID 情報 ID 1 とを、図示しない操作手段を操作して発注者端末装置 3 1 1 に入力する。なお、発注情報  $a 1$  には、受注者 3 3 を特定する情報が含まれている。

次に、図 1 2 に示す発注者端末装置 3 1 1 の暗号化部 3 6 3 は、記憶部 3 6 5 から読み出した所定の暗号鍵を用いて、発注情報  $a 1$  と、個人キー情報  $k 1$  およ

び個人ID情報ID1を暗号化し、当該暗号化した情報を格納した認証要求Inf1（本発明の第1の要求）を、送信部362からネットワークを介して、図11に示すネットワーク銀行340に送信する。

#### 【0131】

##### ステップST32：

図14に示す認証装置350は、発注者端末装置311からの認証要求Inf1を受信部381が受信すると、記憶部385から所定の暗号化鍵を読み出し、復号部384において、当該暗号鍵を用いて認証要求Inf1を復号する。

次に、認証装置350は、制御部386の制御に基づいて、上記復号した認証要求Inf1に格納された発注情報a1に含まれる受注者33を特定する情報b1を格納した要求Inf2（本発明の第2の要求）を、記憶部385から読み出した所定の暗号鍵を用いて暗号化部383で暗号化した後に、受信部381からネットワークを介して認証装置351に送信する。

#### 【0132】

##### ステップST33：

図15に示す認証装置351の制御部396は、認証装置350からの要求Inf2を受信部391が受信すると、記憶部395から読み出した所定の暗号鍵を用いて復号部394において当該要求Inf2を復号する。

次に、署名作成部397は、当該復号された要求Inf2に格納された受注者33を特定する情報b1に対応する受注者33の公開鍵 $K_{33,p}$ を記憶部385から読み出し、当該公開鍵 $K_{33,p}$ について、記憶部385から読み出した自らの秘密鍵 $K_{41,s}$ を用いて自らの認証結果を示す署名情報Au-B（本発明の第1の署名情報）を作成する。

次に、暗号化部393は、受注者33の公開鍵 $K_{33,p}$ および署名情報Au-Bを格納した応答Inf3を、記憶部395から読み出した所定の暗号鍵を用いて暗号化した後に、送信部392からネットワークを介して認証装置350に送信する。

#### 【0133】

##### ステップST34：

図14に示す認証装置350の復号部384は、認証装置351からの応答Inf3を受信部381が受信すると、記憶部385から読み出した所定の暗号鍵を用いて、応答Inf3を復号する。

次に、署名作成部387は、ステップST32で復号した要求Inf1から個人キー情報k1を削除した情報Inf1'と、上記復号された応答Inf3に格納された署名情報Au-Bと、記憶部385から読み出した自らの公開鍵 $K_{40,P}$ とについて、記憶部385から読み出した自らの秘密鍵 $K_{40,S}$ を用いて署名情報Au-A1を作成する。

次に、制御部386は、情報Inf1'と、署名情報Au-Bと、自らの公開鍵 $K_{40,P}$ と、上記生成した署名情報Au-A1とを格納した要求Inf4（本発明の第3の要求）を生成する。

次に、暗号化部383は、ステップST34で認証装置351から受信した受注者33の公開鍵 $K_{33,P}$ を用いて、上記生成した要求Inf4を暗号化した後に、送信部382から、ネットワークを介して受注者端末装置315に送信する。

#### 【0134】

ステップST35：

受注者端末装置315の復号部374は、認証装置350からの要求Inf4を受信部371が受信すると、記憶部375から読み出した自らの秘密鍵 $K_{33,S}$ を用いて、要求Inf4を復号する。

次に、受注者端末装置315の署名検証部377は、上記復号した要求Inf4に格納された署名情報Au-Bを、記憶部375から読み出した認証装置351の公開鍵 $K_{41,P}$ を用いて検証する。また、署名情報検証部は、上記復号した要求Inf4に格納された認証装置350の公開鍵 $K_{40,P}$ を用いて、要求Inf4に格納された署名情報Au-A1を検証する。

#### 【0135】

受注者端末装置315の制御部376は、署名検証部が上記検証の結果、署名情報Au-B、Au-A1の正当性が認証されると、要求Inf4に格納された情報Inf1'と、署名情報Au-B、Au-A1と、自らの個人キー情報Zとを格納した応答Inf5（本発明の所定の応答）を生成する。

次に、受注者端末装置 315 の送信部 372 は、上記生成した応答 Inf 5 を、上記復号した要求 Inf 4 に格納された認証装置 350 の公開鍵  $K_{40,P}$  を用いて復号した後に、送信部 372 から、ネットワークを介して認証装置 350 に送信する。

受注者端末装置 315 によって、署名情報 Au-B, Au-A1 の正当性が認証されると、受注者 33 は、例えば、要求 Inf 4 に格納された情報 Inf 1' 内の発注情報 a1 に基づいて、発注者 31 が発注した商品等を発注者 31 に発送したり、発注者 31 が注文したサービスを発注者 31 に提供する。

#### 【0136】

ステップ ST36 :

認証装置 350 の復号部 384 は、受注者端末装置 315 からの応答 Inf 5 を受信部 381 が受信すると、記憶部 385 から読み出した自らの秘密鍵  $K_{40,S}$  を用いて、Inf 5 を復号し、要求 Inf 1 に格納された発注情報 a1 と、当該復号された Inf 5 に格納された受注者 33 の個人キー情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 385 に格納する。当該履歴情報は、ネットワーク銀行 340 が、発注者 31 に対して決済を行う際に用いられる。

また、認証装置 350 の署名作成部 387 は、ステップ ST32 で受信した要求 Inf 1 と、応答 Inf 5 に含まれる受注者 33 の個人キー情報 Z と、ステップ ST34 で作成した署名情報 Au-A1 とについて、自らの秘密鍵  $K_{40,S}$  を用いて自らの認証結果を示す署名情報 Au-A2 (本発明の第 2 の署名情報) を作成する。

次に、認証装置 350 の制御部 386 は、要求 Inf 1 と、個人キー情報 Z と、署名情報 Au-A1 と、署名情報 Au-A2 とを格納した応答 Inf 6 を作成する。

#### 【0137】

次に、認証装置 350 の暗号化部 383 は、上記作成した応答 Inf 6 を、認証装置 350 から読み出した所定の暗号鍵を用いて暗号化した後に、送信部 382 から、ネットワークを介して発注者端末装置 311 に送信する。

発注者端末装置 311 では、受信した応答 Inf 6 を、図 12 に示す記憶部 3

6 5 から読み出した所定の暗号鍵を用いて復号部 3 6 4 で復号する。

次に、発注者端末装置 3 1 1 の署名検証部 3 6 6 は、当該復号した応答 I n f 6 に格納された署名情報 A u - A 1, A u - A 2 を、記憶部 3 6 5 から読み出したネットワーク銀行 3 4 0 の公開鍵  $K_{40,p}$  を用いて検証することで、受注者端末装置 3 1 5 との間の当該取り引きが正当に認証されたことを確認する。

#### 【 0 1 3 8 】

以上説明したように、トランザクション認証システム 3 0 1 によれば、認証装置 3 5 0 から認証装置 3 5 1 へは、発注者 3 1 の個人キー情報 k 1 および個人 I D 情報 I D 1 を送信しないことから、発注者 3 1 の個人情報が、発注者 3 1 が契約していない他のネットワーク銀行 3 4 1 に漏れることを回避できる。

#### 【 0 1 3 9 】

また、トランザクション認証システム 3 0 1 によれば、認証装置 3 5 0 が、認証装置 3 5 1 から受けた受注者 3 3 の公開鍵  $K_{33,p}$  および署名情報 A u - B を用いて、受注者 3 3 の受注者端末装置 3 1 5 との間で直接通信を行うことで、当該取り引きの履歴を認証装置 3 5 0 に格納できる。

また、トランザクション認証システム 3 0 1 によれば、受注者 3 3 は、自らの契約した認証装置 3 5 0 の署名情報 A u - B を検証することで、当該取り引きの正当性を確認できる。

また、トランザクション認証システム 3 0 1 によれば、認証装置 3 5 0 と 3 5 1 との間では、図 1 6 に示す要求 I n f 2 および I n f 3 を伝送するだけで、発注者 3 1 と受注者 3 3 との間の取り引きを認証でき、認証装置 3 5 0 と 3 5 1 との間の通信量を小さくできる。

#### 【 0 1 4 0 】

また、トランザクション認証システム 3 0 1 によれば、図 1 4 に示す認証装置 3 5 0 の課金処理部 3 8 8 と、図 1 5 に示す認証装置 3 5 1 の課金処理部 3 9 8 との間に通信を行うことで、発注者 3 1 と受注者 3 3 との間の取り引きに関する認証に対して行う課金の割合を柔軟に決定できる。

#### 【 0 1 4 1 】

上述したように、トランザクション認証システム 3 0 1 によれば、異なる認証

機関と契約をしている複数の取り引き者の間の取り引きに関する認証を、高い信頼性で、しかも効率的に行うことができる。その結果、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

#### 【0142】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ネットワーク銀行340、341が、それぞれ認証装置350、351を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行340、341とは別の機関が、認証装置350、351を用いてトランザクションの認証業務を行うようにしてもよい。

#### 【0143】

また、上述した実施形態では、発注者31が契約したネットワーク銀行340の認証装置350と、受注者33が契約したネットワーク銀行341の認証装置351との間で連携して認証処理を行う場合を例示したが、3人以上の取り引き者がそれぞれ異なる認証機関と契約を行っている場合に、3以上の認証装置間で連携して認証処理を行う場合にも、本発明は適用可能である。

#### 【0144】

また、上述した実施形態では、図16に示すステップST31のように、暗号化された発注情報a1と、個人キー情報k1および個人ID情報ID1とを含む認証要求Inf1を、発注者端末装置311から認証装置350に送信する場合を例示したが、発注情報a1および個人キー情報k1を含む認証要求Inf1を、発注者端末装置311から認証装置350に送信してもよい。このようにすれば、課金に係わる情報である個人ID情報ID1はネットワークを介して伝送されないため、ネットワーク上で個人ID情報ID1が不正に取得され、悪用されることを回避できる。

#### 【0145】

また、本発明では、例えば、認証装置350から受注者端末装置315に、署名情報Au-A2（本発明の第2の署名情報）を送信するようにしてもよい。

【 0 1 4 6 】

第 4 実施形態

図 1 7 は、本実施形態の情報記録装置 6 0 1 の構成図である。

図 1 7 に示すように、情報記録装置 6 0 1 は、読み出し回路 6 1 0、暗号化回路 6 1 1、情報分割回路 6 1 2、書き込み回路 6 1 3、6 1 4 を有する。

本実施形態は、第 2 1、2 3 および 2 5 の発明に対応した実施形態である。

情報記録装置 6 0 1 は、記録媒体 6 1 5 から読み出した個人情報 D 1 を暗号化した後に、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 3、D 4 に分割し、モジュール D 3 を記録媒体 6 1 6 に書き込み、モジュール D 4 を記録媒体 6 1 7 に書き込む。

本実施形態において、記録媒体 6 1 5、6 1 6、6 1 7 は、HDD 装置や、携帯性のある CD-ROM、フロッピーディスク、PC カードなどの記録媒体である。

【 0 1 4 7 】

読み出し回路 6 1 0 は、記録媒体 6 1 5 から読み出した個人情報 D 1 を暗号化回路 6 1 1 に出力する。

個人情報 D 1 は、図 1 8 に示すように、情報 Data 1 ~ Data N からなる。また、個人情報 D 1 は、例えば、ユーザの個人 ID 情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

【 0 1 4 8 】

暗号化回路 6 1 1 は、所定の暗号鍵を用いて、読み出し回路 6 1 0 から入力した個人情報 D 1 を暗号化して個人情報 D 2 を生成し、これを情報分割回路 6 1 2 に出力する。

暗号化された個人情報 D 2 は、図 1 8 に示すように、それぞれ情報 Data 1 ~ Data N を暗号化した情報 Data 1' ~ Data N' からなる。

【 0 1 4 9 】

情報分割回路 6 1 2 は、暗号化回路 6 1 1 から入力した暗号化された個人情報 D 2 を、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール

ルD3、D4に分割し、モジュールD3を書き込み回路613に出力し、モジュールD4を書き込み回路614に出力する。

図18に示すように、情報分割回路612は、情報D2内の情報Data1'～DataN'を、それぞれ情報Data1A'およびData1B'、情報Data2A'およびData2B'、情報Data3A'およびData3B'、.....、情報DataKA'およびDataKB'、.....、情報DataNA'およびDataNB'に分割する。

そして、情報分割回路612は、情報Data1A'、Data2A'、Data3A'、.....、DataKA'、.....、DataNA'からなるモジュールD3を書き込み回路613に出力する。

また、情報分割回路612は、情報Data1B'、Data2B'、Data3B'、.....、DataKB'、.....、DataNB'からなるモジュールD4を書き込み回路614に出力する。

#### 【0150】

書き込み回路613は、情報分割回路612から入力したモジュールD3を記録媒体616に書き込む。

#### 【0151】

書き込み回路614は、情報分割回路612から入力したモジュールD4を記録媒体617に書き込む。

#### 【0152】

以下、情報記録装置601の動作を説明する。

図19は、情報記録装置601の動作を説明するためのフローチャートである。

#### 【0153】

ステップST81:

読み出し回路610によって、記録媒体615から図18に示す個人情報D1が読み出されて暗号化回路611に出力される。

#### 【0154】

ステップST82:



暗号化回路 611 において、所定の暗号鍵を用いて、読み出し回路 610 から入力された個人情報 D1 が暗号化されて図 18 に示す個人情報 D2 が生成され、当該個人情報 D2 が情報分割回路 612 に出力される。

#### 【0155】

ステップ ST83 :

情報分割回路 612 において、暗号化回路 611 から入力された個人情報 D2 が、それぞれを単独では個人情報 D1 の秘匿性が保持される図 18 に示す 2 つのモジュール D3, D4 に分割される。

そして、情報分割回路 612 から書き込み回路 613 にモジュール D3 が出力され、情報分割回路 612 から書き込み回路 614 にモジュール D4 が出力される。

#### 【0156】

ステップ ST84 :

書き込み回路 613 によって、モジュール D3 が記録媒体 616 に書き込まれる。

書き込み回路 614 によって、モジュール D4 が記録媒体 617 に書き込まれる。

#### 【0157】

以上説明したように、情報記録装置 601 によれば、図 18 に示すように、個人情報 D1 が、暗号化された後に、それぞれを単独では個人情報 D1 の秘匿性が保持される 2 つのモジュール D3, D4 に分割され、モジュール D3, D4 がそれぞれ物理的に独立した記録媒体 616, 617 にそれぞれ記録される。

そのため、記録媒体 616, 617 を別々に保管すれば、記録媒体 616, 617 の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報 D1 の秘匿性は保たれる。

#### 【0158】

### 第5実施形態

図 20 は、本実施形態の情報復元装置 631 の構成図である。

情報復元装置 6 3 1 は、上述した第 4 実施形態の情報記録装置 6 0 1 によって、記録媒体 6 1 6 と 6 1 7 とに分割して記録された個人情報から、本来の個人情報 D 1 を復元する。

本実施形態は、第 2 2 および 2 4 の発明に対応した実施形態である。

図 2 0 に示すように、情報復元装置 6 3 1 は、読み出し回路 6 2 0、6 2 1、情報合成回路 6 2 2、復号回路 6 2 3 および書き込み回路 6 2 4 を有する。

図 2 0 において、記録媒体 6 1 6 および 6 1 7 には、前述した第 4 実施形態で説明した図 1 9 に示す処理を経て、それぞれモジュール D 3 および D 4 が記録されている。

#### 【0 1 5 9】

読み出し回路 6 2 0 は、記録媒体 6 1 6 から読み出したモジュール D 3 を情報合成回路 6 2 2 に出力する。

#### 【0 1 6 0】

読み出し回路 6 2 1 は、記録媒体 6 1 7 から読み出したモジュール D 4 を情報合成回路 6 2 2 に出力する。

#### 【0 1 6 1】

情報合成回路 6 2 2 は、図 2 1 に示すように、読み出し回路 6 2 0 から入力したモジュール D 3 と、読み出し回路 6 2 1 から入力したモジュール D 4 とを合成して個人情報 D 2 を生成し、これを復号回路 6 2 3 に出力する。

#### 【0 1 6 2】

復号回路 6 2 3 は、情報合成回路 6 2 2 から入力した個人情報 D 2 を、所定の復号鍵を用いて復号して個人情報 D 1 を生成し、これを書き込み回路 6 2 4 に出力する。

#### 【0 1 6 3】

書き込み回路 6 2 4 は、復号回路 6 2 3 から入力した個人情報 D 1 を、記録媒体 6 1 5 に書き込む。

#### 【0 1 6 4】

以下、情報復元装置 6 3 1 の動作を説明する。

図 2 2 は、情報復元装置 6 3 1 の動作を説明するためのフローチャートである

## 【0165】

## ステップST91:

読み出し回路620によって、記録媒体616から図21に示すモジュールD3が読み出されて情報合成回路622に出力される。

また、読み出し回路621によって、記録媒体617から図21に示すモジュールD4が読み出されて情報合成回路622に出力される。

## 【0166】

## ステップST92:

情報合成回路622において、図21に示すように、読み出し回路620から入力したモジュールD3と、読み出し回路621から入力したモジュールD4とが合成されて個人情報D2が生成される。

個人情報D2は、情報合成回路622から復号回路623に出力される。

## 【0167】

## ステップST93:

復号回路623において、情報合成回路622から入力した個人情報D2が、所定の復号鍵を用いて復号して個人情報D1を生成され、これ書き込み回路624に出力される。

## 【0168】

## ステップST94:

書き込み回路624によって、復号回路623から入力した個人情報D1が記録媒体615に書き込まれる。

## 【0169】

以上説明したように、情報復元装置631によれば、正当な者が当該装置を用いることで、前述した第4実施形態の情報記録装置601によって別々の記録媒体616、617に格納されたモジュールD3、D4から個人情報D1を復元できる。

## 【0170】

第6実施形態

図 2 3 は、本実施形態の情報記録装置 6 4 1 の構成図である。

図 2 3 に示すように、情報記録装置 6 4 1 は、読み出し回路 6 5 0、情報分割回路 6 5 1、暗号化回路 6 5 2、6 5 3 および書き込み回路 6 5 4、6 5 5 を有する。

本実施形態は、第 2 1、2 3 および 2 5 の発明に対応した実施形態である。

情報記録装置 6 4 1 は、記録媒体 6 1 5 から読み出した個人情報 D 1 を、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 1 2、D 1 3 に分割した後に暗号化してモジュール D 1 4、D 1 5 を生成し、モジュール D 1 4 を記録媒体 6 1 6 に書き込み、モジュール D 1 5 を記録媒体 6 1 7 に書き込む。

#### 【0 1 7 1】

読み出し回路 6 5 0 は、記録媒体 6 1 5 から読み出した個人情報 D 1 を情報分割回路 6 5 1 に出力する。

個人情報 D 1 は、図 2 4 に示すように、情報 Data 1 ~ Data N からなる。また、個人情報 D 1 は、例えば、ユーザの個人 ID 情報や暗証番号、取り引きの履歴情報、ユーザの名前、住所、経歴および職業などの秘匿性のある情報である。

#### 【0 1 7 2】

情報分割回路 6 5 1 は、読み出し回路 6 5 0 から入力した個人情報 D 1 を、それぞれを単独では個人情報 D 1 の秘匿性が保持される 2 つのモジュール D 1 2、D 1 3 に分割し、モジュール D 1 2 を暗号化回路 6 5 2 に出力し、モジュール D 1 3 を暗号化回路 6 5 3 に出力する。

図 2 4 に示すように、情報分割回路 6 5 1 は、情報 D 1 内の情報 Data 1 ~ Data N を、それぞれ情報 Data 1 A および Data 1 B、情報 Data 2 A および Data 2 B、情報 Data 3 A および Data 3 B、...、情報 Data K A および Data K B、...、情報 Data N A および Data N B に分割する。

そして、情報分割回路 6 5 1 は、情報 Data 1 A、Data 2 A、Data 3 A、...、Data K A、...、Data N A からなるモジュール D 1 2

を暗号化回路652に出力する。

また、情報分割回路651は、情報Data1B, Data2B, Data3B, . . . , DataKB, . . . , DataNBからなるモジュールD13を暗号化回路653に出力する。

【0173】

暗号化回路652は、所定の暗号鍵を用いて、情報分割回路651から入力した個人情報D12を暗号化して個人情報D14を生成し、これを書き込み回路654に出力する。

暗号化された個人情報D14は、図24に示すように、それぞれ情報Data1A~DataNAを暗号化した情報Data1A'~DataNA'からなる。

【0174】

暗号化回路653は、所定の暗号鍵を用いて、情報分割回路651から入力した個人情報D13を暗号化して個人情報D15を生成し、これを書き込み回路655に出力する。暗号化回路653が用いる暗号鍵は、暗号化回路652が用いる暗号鍵と同じものを用いてもよいし、異なるものを用いてもよい。

暗号化された個人情報D15は、図24に示すように、それぞれ情報Data1B~DataNBを暗号化した情報Data1B'~DataNB'からなる。

【0175】

書き込み回路654は、暗号化回路652から入力したモジュールD14を記録媒体616に書き込む。

【0176】

書き込み回路655は、暗号化回路653から入力したモジュールD15を記録媒体617に書き込む。

【0177】

以下、情報記録装置601の動作を説明する。

図25は、情報記録装置641の動作を説明するためのフローチャートである。

【0178】

ステップST131:

読み出し回路650によって、記録媒体615から図24に示す個人情報D1が読み出されて情報分割回路651に出力される。

【0179】

ステップST132:

情報分割回路651において、図24に示すように、読み出し回路650から入力した個人情報D1が、それぞれを単独では個人情報D1の秘匿性が保持される2つのモジュールD12, D13に分割され、モジュールD12が暗号化回路652に出力され、モジュールD13が暗号化回路653に出力される。

【0180】

ステップST133:

暗号化回路652において、図24に示すように、所定の暗号鍵を用いて、情報分割回路651から入力した個人情報D12が暗号化されて個人情報D14が生成され、これが書き込み回路654に出力される。

また、暗号化回路653において、図24に示すように、所定の暗号鍵を用いて、情報分割回路651から入力した個人情報D13が暗号化されて個人情報D15が生成され、これが書き込み回路655に出力される。

【0181】

ステップST134:

書き込み回路654によって、暗号化回路652から入力したモジュールD14が記録媒体616に書き込まれる。

書き込み回路655によって、暗号化回路653から入力したモジュールD15が記録媒体617に書き込まれる。

【0182】

以上説明したように、情報記録装置641によれば、図24に示すように、個人情報D1が、それぞれを単独では個人情報D1の秘匿性が保持される2つのモジュールD12, D13に分割された後に暗号化されてモジュールD14, D15が生成され、モジュールD14, D15がそれぞれ物理的に独立した記録媒体

6 1 6, 6 1 7 にそれぞれ記録される。

そのため、記録媒体 6 1 6, 6 1 7 を別々に保管すれば、記録媒体 6 1 6, 6 1 7 の一方が盗難され、しかも、盗難された記録媒体に記録されているモジュールの復号が盗難者によって行われた場合でも、個人情報 D 1 の秘匿性は保たれる。

#### 【0 1 8 3】

##### 第 7 実施形態

図 2 6 は、本実施形態の情報復元装置 6 6 1 の構成図である。

情報復元装置 6 6 1 は、上述した第 6 実施形態の情報記録装置 6 4 1 によって、記録媒体 6 1 6 と 6 1 7 とに分割して記録された個人情報から、本来の個人情報 D 1 を復元する。

図 2 6 に示すように、情報復元装置 6 6 1 は、読み出し回路 6 7 0, 6 7 1、復号回路 6 7 2, 6 7 3、情報合成回路 6 7 4 および書き込み回路 6 7 5 を有する。

本実施形態は、第 2 2 および第 2 4 の発明に対応した実施形態である。

図 2 6 において、記録媒体 6 1 6 および 6 1 7 には、前述した第 6 実施形態で説明した図 2 5 に示す処理を経て、それぞれモジュール D 1 4 および D 1 5 が記録されている。

#### 【0 1 8 4】

読み出し回路 6 7 0 は、記録媒体 6 1 6 から読み出したモジュール D 1 4 を復号回路 6 7 2 に出力する。

#### 【0 1 8 5】

読み出し回路 6 7 1 は、記録媒体 6 1 7 から読み出したモジュール D 1 5 を復号回路 6 7 3 に出力する。

#### 【0 1 8 6】

復号回路 6 7 2 は、読み出し回路 6 7 0 から入力したモジュール D 1 4 を、所定の復号鍵を用いて復号してモジュール D 1 2 を生成し、これを情報合成回路 6 7 4 に出力する。

#### 【0 1 8 7】

復号回路673は、読み出し回路671から入力したモジュールD15を、所定の復号鍵を用いて復号してモジュールD13を生成し、これを情報合成回路674に出力する。

【0188】

情報合成回路674は、図27に示すように、復号回路672から入力したモジュールD12と、復号回路673から入力したモジュールD13とを合成して個人情報D1を生成し、これを書き込み回路675に出力する。

【0189】

書き込み回路675は、情報合成回路674から入力した個人情報D1を、記録媒体615に書き込む。

【0190】

以下、情報復元装置661の動作を説明する。

図28は、情報復元装置661の動作を説明するためのフローチャートである。  
。 ステップST141：

読み出し回路670によって、図27に示すように、記録媒体616からモジュールD14が読み出されて復号回路672に出力される。

また、読み出し回路671によって、記録媒体617からモジュールD15が読み出されて復号回路673に出力される。

【0191】

ステップST142：

復号回路672において、読み出し回路670から入力したモジュールD14が、所定の復号鍵を用いて復号されてモジュールD12が生成され、これが情報合成回路674に出力される。

また、復号回路673において、読み出し回路671から入力したモジュールD15が、所定の復号鍵を用いて復号されてモジュールD13が生成され、これが情報合成回路674に出力される。

【0192】

ステップST143：

情報合成回路674において、図27に示すように、復号回路672から入力



したモジュールD12と、復号回路673から入力したモジュールD13とが合成されて個人情報D1が生成され、これを書き込み回路675に出力される。

【0193】

ステップST144：

書き込み回路675によって、情報合成回路674から入力された個人情報D1が、記録媒体615に書き込まれる。

【0194】

以上説明したように、情報復元装置631によれば、正当な者が当該装置を用いることで、前述した第6実施形態の情報記録装置641によって別々の記録媒体616、17に格納されたモジュールD14、D15から個人情報D1を復元できる。

【0195】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、個人情報を分割して得た複数のモジュールを異なる記録媒体に記録する場合を例示したが、当該複数のモジュールを同じ記録媒体の異なる領域に記録してもよい。この場合に、記録媒体の何れの領域に何れもモジュールを記録したかを秘密にしておけば、当該記録媒体を不正に取得した者は、記録媒体から読み出したモジュールの合成の仕方が分からず、個人情報を復元できない。

【0196】

また、上述した実施形態では、所定の情報を分割する前後の何れか一方で暗号化を行う場合を例示したが、所定の情報を分割する前後の何れでも暗号化を行う場合、並びに所定の情報を分割する前後の双方で暗号化を行う場合でも本発明は適用可能である。

【0197】

また、上述した実施形態では、本発明の所定の情報として、個人情報を例示したが、その他、映像、音声などの情報であってもよい。

【0198】

また、上述した実施形態では、個人情報を2分割して2つの記録媒体616、

6 1 7 に記録する場合を例示したが、個人情報 を 3 分割以上して 3 つ以上の記録媒体に記録してもよい。

【 0 1 9 9 】

#### 第 8 実施形態

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図 2 9 は、本実施形態のトランザクション認証システム 2 0 1 の全体構成図である。

図 2 9 に示すように、トランザクション認証システム 2 0 1 では、例えば、発注者 3 1 の発注者端末装置 2 1 1 と、受注者 3 3 の受注者端末装置 2 1 5 と、ネットワーク銀行 2 4 0 の認証装置 2 5 0 と、認証履歴を格納する認証履歴格納装置 1 4 とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者 3 1 と受注者 3 3 との間のトランザクション（取引）の正当性を認証装置 2 5 0 で認証する。

なお、当該ネットワークに接続されている発注者端末装置 2 1 1 および発注者受注者端末装置 2 1 5 の数は任意である。

【 0 2 0 0 】

本実施形態は、第 7 ～ 第 1 1 の発明に対応した実施形態である。

発注者端末装置 2 1 1 が第 9 の発明の処理装置に対応し、認証装置 2 5 0 が本発明の認証装置に対応している。

【 0 2 0 1 】

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 2 4 0 との間で認証を行うことに関する契約が成されている。また、発注者 3 1 と引き落とし銀行 2 4 2 との間では、例えば、ネットワーク銀行 2 4 0 によって認証された取引に関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 2 4 0 と保険会社 2 4 3 との間では、ネットワーク銀行 2 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

【 0 2 0 2 】

以下、トランザクション認証システム 2 0 1 を構成する各装置について説明する。

〔発注者端末装置 2 1 1〕

図 3 0 に示すように、発注者端末装置 2 1 1 は、例えば、発注者 3 1 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 2 6 1、送信部 2 6 2、暗号化部 2 6 3、復号部 2 6 4、記憶部 2 6 5、制御部 2 6 6 および署名検証部 2 6 7 を有する。

なお、発注者端末装置 2 1 1 は、例えば、発注者 3 1 が使用する際に、発注者 3 1 の指紋等の身体的特徴から得られる情報と、予め記憶部 2 6 5 に予め記憶してある身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な利用者であることを認証する生体認証部を有していてもよい。

【0 2 0 3】

ここで、受信部 2 6 1 が第 9 の発明の受信手段に対応し、送信部 2 6 2 が第 9 の発明の送信手段に対応し、制御部 2 6 6 が第 9 の発明の制御手段に対応している。

【0 2 0 4】

受信部 2 6 1 は、ネットワークを介して認証装置 2 5 0 から情報あるいは要求を受信する。

送信部 2 6 2 は、ネットワークを介して認証装置 2 5 0 に情報あるいは要求を送信する。

また、受信部 2 6 1 および送信部 2 6 2 は、受注者 3 3 が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 2 6 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 2 6 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 2 6 5 は、製造元で受注者端末装置 2 1 5 に付された装置 ID 情報  $ID_M$ （本発明の装置識別情報）と、発注者 3 1 が作成した秘密鍵  $K_{33,S}$  などを格納する。

署名検証部 2 6 7 は、例えば、認証装置 2 5 0 が作成した署名情報を、ネット

ワーク銀行 2 4 0 の公開鍵  $K_{40,P}$  を用いて検証する。

制御部 2 6 6 は、発注者端末装置 2 1 1 内の各構成要素の処理を統括的に制御する。

#### 【 0 2 0 5 】

制御部 2 6 6 は、例えば、発注者 3 1 による操作に応じて、発注情報  $a 1$  と、個人キー情報  $k 1$ （本発明の個人識別情報）と、個人 ID 情報  $ID 1$ （本発明の個人識別情報）と、記憶部 2 6 5 から読み出した装置 ID 情報  $ID_M$  との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求  $Inf 1$  を生成する。

また、制御部 2 6 6 は、例えば、認証要求  $Inf 1$  を認証装置 2 5 0 に送信した後に、認証装置 2 5 0 から認証応答  $Inf 4$  を受信したときに、認証応答  $Inf 4$  に含まれる認証要求の送信元の装置を示す装置 ID 情報  $ID_M$  と、記憶部 2 6 5 から読み出した発注者端末装置 2 1 1 の装置 ID 情報  $ID_M$  とが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置 2 1 5 および認証装置 2 5 0 の少なくとも一方に通知する。

#### 【 0 2 0 6 】

##### 〔受注者端末装置 2 1 5〕

図 3 1 に示すように、受注者端末装置 2 1 5 は、サイバーモール (Cyber Mall) などに店舗を出している受注者 3 3 が使用するサーバ装置であり、受信部 2 7 1、送信部 2 7 2、暗号化部 2 7 3、復号部 2 7 4、記憶部 2 7 5、制御部 2 7 6 および署名検証部 2 7 7 を有する。

受信部 2 7 1 は、ネットワークを介して認証装置 2 5 0 から情報あるいは要求を受信する。

送信部 2 7 2 は、ネットワークを介して認証装置 2 5 0 に情報あるいは要求を送信する。

また、受信部 2 7 1 および送信部 2 7 2 は、発注者端末装置 2 1 1 からのアクセスに応じて、例えば、記憶部 2 7 5 から読み出した受注者 3 3 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 2 1 1 に送信する。

暗号化部 273 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 274 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 275 は、受注者 33 が作成した秘密鍵  $K_{33,S}$  などを格納する。

制御部 276 は、受注者端末装置 215 内の各構成要素の処理を統括的に制御する。

署名検証部 277 は、例えば、ネットワーク銀行 240 の公開鍵  $K_{40,P}$  を用いて、認証装置 250 が作成した署名情報の検証を行う。

#### 【0207】

##### 〔認証装置 250〕

図 32 に示すように、認証装置 250 は、受信部 281、送信部 282、暗号化部 283、復号部 284、記憶部 285、制御部 286、署名作成部 287 および課金処理部 288 を有する。

#### 【0208】

ここで、受信部 281 が第 7 および第 8 の発明の受信手段に対応し、送信部 282 が第 7 および第 8 の発明の送信手段に対応し、記憶部 285 が第 7 および第 8 の発明の記憶手段に対応し、制御部 286 が第 7 および第 8 の発明の認証処理手段に対応している。

#### 【0209】

受信部 281 は、ネットワークを介して発注者端末装置 211 および受注者端末装置 215 から情報あるいは要求を受信する。

送信部 282 は、ネットワークを介して発注者端末装置 211 および受注者端末装置 215 に情報あるいは要求を送信する。

暗号化部 283 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 284 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 285 は、発注者 31 がネットワーク銀行 240 と契約したときに、発注者 31 の個人キー情報  $k_1$  と、個人 ID 情報  $ID_1$  と、発注者端末装置 211 のアドレス（または、発注者端末装置 211 が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を記憶する。また、記憶部 285 は、例えば、発注者 31 および受注者 33 がネットワーク銀行 240 と

契約をしたときに、発注者 3 1 が作成した秘密鍵  $K_{31,S}$  に対応する公開鍵  $K_{31,P}$ 、並びに受注者 3 3 が作成した秘密鍵  $K_{33,S}$  に対応する公開鍵  $K_{33,P}$  などを格納する。

制御部 2 8 6 は、認証装置 2 5 0 内の各構成要素の処理を統括的に制御する。

署名作成部 2 8 7 は、ネットワーク銀行 2 4 0 の秘密鍵  $K_{40,S}$  を用いて署名情報の作成を行う。

課金処理部 2 8 8 は、発注者 3 1 による取引に関する認証に対しての課金処理を行う。

認証装置 2 5 0 の各構成要素の詳細な処理については、後述する動作例で記載する。

#### 【 0 2 1 0 】

以下、トランザクション認証システム 2 0 1 の動作例を説明する。

当該動作例を開始する前提として、発注者 3 1 とネットワーク銀行 2 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 2 4 0 は、発注者 3 1 に対して、個人キー情報  $k 1$  および個人 ID 情報  $ID 1$  を発行する。

ネットワーク銀行 2 4 0 は、個人キー情報  $k 1$  と、個人 ID 情報  $ID 1$  と、発注者端末装置 2 1 1 のアドレス（または、発注者端末装置 2 1 1 が配設された家庭のセット・トップ・ボックスのアドレスあるいは電話番号等）との対応表を図 3 2 に示す認証装置 2 5 0 の記憶部 2 8 5 に記憶する。ここで、個人キー情報  $k 1$  は、例えば、ネットワーク銀行 2 4 0 と契約した契約者（発注者 3 1）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報  $ID 1$  は、発注者 3 1 の銀行口座番号などの課金に係わる情報を示す識別子である。

#### 【 0 2 1 1 】

また、ネットワーク銀行 2 4 0 は、自らの秘密鍵  $K_{40,S}$  を図 3 2 に示す認証装置 2 5 0 の記憶部 2 8 5 に記憶すると共に、当該秘密鍵  $K_{40,S}$  に対応する公開鍵  $K_{40,P}$  を発注者端末装置 2 1 1 および受注者端末装置 2 1 5 に送信する。発注者端末装置 2 1 1 は、公開鍵  $K_{40,P}$  を図 3 0 に示す記憶部 2 6 5 に記憶する。受注者端末装置 2 1 5 は、公開鍵  $K_{40,P}$  を図 3 1 に示す記憶部 2 7 5 に記憶する。

#### 【 0 2 1 2 】

また、受注者 3 3 とネットワーク銀行 2 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 2 4 0 は、受注者 3 3 に対して、個人キー情報 Z および個人 ID 情報 ID 2 を発行する。ネットワーク銀行 2 4 0 は、個人キー情報 Z および個人 ID 情報 ID 2 の対応表を図 3 2 に示す認証装置 2 5 0 の記憶部 2 8 5 に記憶する。

### 【 0 2 1 3 】

図 3 3 は、トランザクション認証システム 2 0 1 の動作例を説明するための図である。

#### ステップ ST 2 1 :

図 2 9 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、発注者 3 1 の個人キー情報 k 1 と、発注者 3 1 の個人 ID 情報 ID 1 とを、図示しない操作手段を操作して発注者端末装置 2 1 1 に入力する。なお、発注情報 a 1 には、受注者 3 3 を特定する情報が含まれている。

次に、図 3 0 に示す発注者端末装置 2 1 1 の暗号化部 2 6 3 は、記憶部 2 6 5 から読み出したネットワーク銀行 2 4 0 の公開鍵  $K_{40,P}$  を用いて、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、記憶部 2 6 5 から読み出した装置 ID 情報 ID<sub>M</sub> との全体に対してを暗号化を行い、当該暗号化した情報を格納した認証要求 Inf 1 (本発明の第 1 の要求) を、送信部 2 6 2 からネットワークを介して、図 2 9 に示すネットワーク銀行 2 4 0 の認証装置 2 5 0 に送信する。

### 【 0 2 1 4 】

#### ステップ ST 2 2 :

図 3 2 に示す認証装置 2 5 0 は、発注者端末装置 2 1 1 からの認証要求 Inf 1 を受信部 2 8 1 が受信すると、記憶部 2 8 5 からネットワーク銀行 2 4 0 の秘密鍵  $K_{40,S}$  を読み出し、復号部 2 8 4 において、当該秘密鍵  $K_{40,S}$  を用いて認証要求 Inf 1 を復号する。

次に、認証装置 2 5 0 は、制御部 2 8 6 の制御に基づいて、上記復号した認証要求 Inf 1 から個人キー情報 k 1 を削除した情報 Inf 1' について、記憶部

285から読み出した自らの秘密鍵 $K_{40,S}$ を用いて署名情報 $Au1$ を作成する。

次に、認証装置250は、情報 $Inf1'$ および署名情報 $Au1$ を格納した要求 $Inf2$ を生成する。

次に、暗号化部283は、図32に示す記憶部285から読み出した受注者33の公開鍵 $K_{33,P}$ を用いて、上記生成した要求 $Inf2$ を暗号化した後に、送信部282から、ネットワークを介して受注者端末装置215に送信する。

#### 【0215】

ステップST23：

受注者端末装置215の復号部274は、認証装置250からの要求 $Inf2$ を受信部271が受信すると、記憶部275から読み出した自らの秘密鍵 $K_{33,S}$ を用いて、要求 $Inf2$ を復号する。

次に、受注者端末装置215の署名検証部277は、上記復号した要求 $Inf2$ に格納された署名情報 $Au1$ を、記憶部275から読み出した認証装置250の公開鍵 $K_{40,P}$ を用いて検証する。

#### 【0216】

受注者端末装置215の制御部276は、署名検証部が上記検証の結果、署名情報 $Au1$ の正当性が認証されると、要求 $Inf2$ に格納された情報 $Inf1'$ を図31に示す記憶部275に記憶する。受注者33は、情報 $Inf1'$ 内の発注情報 $a1$ に基づいて、発注者31への商品等の発送予定などを示す受注確認情報 $c1$ を生成する。

次に、制御部276は、要求 $Inf2$ 、受注確認情報 $c1$ および自らの個人キー情報 $Z$ を格納した応答 $Inf3$ を生成する。

次に、受注者端末装置215の送信部272は、上記生成した応答 $Inf3$ を、記憶部275から読み出したネットワーク銀行240の公開鍵 $K_{40,P}$ を用いて暗号化部273で暗号化した後に、送信部272から、ネットワークを介して認証装置250に送信する。

受注者33は、例えば、要求 $Inf2$ に格納された情報 $Inf1'$ 内の発注情報 $a1$ に基づいて、発注者31が発注した商品等を発注者31に発送したり、発注者31が注文したサービスを発注者31に提供する。



## 【0217】

## ステップST24:

認証装置250の復号部284は、受注者端末装置215からの応答Inf3を受信部281が受信すると、記憶部285から読み出した自らの秘密鍵 $K_{40,S}$ を用いて、Inf3を復号し、要求Inf1に格納された発注情報a1と、当該復号されたInf3に格納された受注者33の個人キー情報Zとを用いて、所定の取り引き履歴情報を作成し、これを記憶部285に格納する。当該履歴情報は、ネットワーク銀行240が、発注者31に対して決済を行う際に用いられる。

また、認証装置250の署名作成部287は、ステップST23で受信した応答Inf3について、自らの秘密鍵 $K_{40,S}$ を用いて署名情報Au2を作成する。

次に、認証装置250の制御部286は、応答Inf3および署名情報Au2を格納した認証応答Inf4を作成する。

次に、認証装置250の暗号化部283は、上記作成し認証した応答Inf4を、記憶部285から読み出した発注者31の公開鍵 $K_{31,P}$ を用いて暗号化した後に、送信部282から、ネットワークを介して発注者端末装置211に送信する。

## 【0218】

## ステップST25:

発注者端末装置211では、受信した認証応答Inf4を、図30示す記憶部265から読み出した発注者31の秘密鍵 $K_{31,S}$ を用いて復号部264で復号する。

次に、発注者端末装置211の署名検証部266は、当該復号した認証応答Inf4に格納された署名情報Au2を、記憶部265から読み出したネットワーク銀行240の公開鍵 $K_{40,P}$ を用いて検証すると共に、Inf4内の発注情報a1内に記述された装置ID情報 $ID_M$ が図30に示す発注者端末装置211の記憶部265に記憶されている自らの装置ID情報 $ID_M$ と一致するかを判断し、一致すると判断した場合には、受注者33との間の当該取り引きが正当に行われたことを確認する。発注者端末装置211は、Inf4内の発注情報a1内に記述された装置ID情報 $ID_M$ が図30に示す発注者端末装置211の記憶部2

65に記憶されている自らの装置ID情報ID<sub>M</sub>と一致しないと判断した場合には、例えば、認証応答Inf4を格納した不正発注通知Inf5を認証装置250および受注者端末装置215の少なくとも一方に送信する。

これにより、認証装置250および受注者端末装置215は、発注者端末装置211が発した認証要求Inf1に対応した発注を取り消す。

また、発注者端末装置211は、不正発生通知Inf5を、図29に示す引き落とし銀行242に送信してもよい。

#### 【0219】

以上説明したように、トランザクション認証システム201によれば、認証要求Inf1内に、個人ID情報ID1の他に当該認証要求を出した装置ID情報ID<sub>M</sub>を自動的に挿入し、認証装置250において、認証要求Inf1に含まれる発注者31が使用する発注者端末装置211のアドレスに、認証結果を含む認証応答Inf4を送信し、当該認証応答Inf4内に当該認証要求を出した装置ID情報ID<sub>M</sub>を格納することで、発注者端末装置211では、認証応答Inf4に格納された当該認証要求を出した装置ID情報ID<sub>M</sub>と自らの装置ID情報ID<sub>M</sub>とが一致するか否かを判断することで、自らの個人ID情報ID1を用いた不正な認証要求（なりすまし）が発生したことを検出できる。

その結果、トランザクション認証システム201によれば、他人の個人ID情報を用いた不正な取り引きを効果的に抑制できる。

#### 【0220】

上述したように、トランザクション認証システム1201によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

#### 【0221】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、発注者端末装置211において、認証応答Inf4内の発注情報a1内に記述された装置ID情報ID<sub>M</sub>が図30に示す発注者端末装置211の記憶部265に記憶されている自らの装置ID情報ID<sub>M</sub>と

一致するかを判断し、一致しないと判断した場合には、例えば、認証応答  $I n f 4$  を格納した不正発注通知  $I n f 5$  を認証装置 2 5 0 および受注者端末装置 2 1 5 の少なくとも一方に送信する場合を例示したが、例えば、一致しない旨（不正な取り引きが行われた旨）を発注者端末装置 2 1 1 のディスプレイなどに表示し、発注者 3 1 にその旨を知らせるようにしてもよい。

また、発注者端末装置 2 1 1 において、上述した装置 ID 情報  $I D_M$  の一致を判断するのではなく、発注者 3 1 が判断してもよい。

また、発注者端末装置 2 1 1 が配設された家庭にホーム・ゲートウェイ (Home Gateway) が設置されている場合には、ホーム・ゲートウェイに発注者端末装置 2 1 1 の装置 ID 情報  $I D_M$  を登録しておき、認証装置 2 5 0 からの認証応答  $I n f 4$  をホーム・ゲートウェイが受信したときに、ホーム・ゲート・ウェイにおいて、上記装置 ID 情報  $I D_M$  の一致の判断を行ってもよい。

#### 【 0 2 2 2 】

また、上述した実施形態では、ネットワーク銀行 2 4 0 が、認証装置 2 5 0 を用いて、トランザクション（取り引き）の認証業務を行う場合を例示したが、ネットワーク銀行 2 4 0 とは別の機関が、認証装置 2 5 0 を用いてトランザクションの認証業務を行うようにしてもよい。

#### 【 0 2 2 3 】

また、上述した実施形態では、図 3 3 に示すステップ S T 2 1 のように、暗号化された発注情報  $a 1$  と、個人キー情報  $k 1$  と、個人 ID 情報  $I D 1$  と、装置 ID 情報  $I D_M$  とを含む認証要求  $I n f 1$  を、発注者端末装置 2 1 1 から認証装置 2 5 0 に送信する場合を例示したが、発注情報  $a 1$  と、個人キー情報  $k 1$  と、装置 ID 情報  $I D_M$  とを含む認証要求  $I n f 1$  を、発注者端末装置 2 1 1 から認証装置 2 5 0 に送信してもよい。このようにすれば、課金に係わる情報である個人 ID 情報  $I D 1$  はネットワークを介して伝送されないため、ネットワーク上で個人 ID 情報  $I D 1$  が不正に取得され、悪用されることを回避できる。

#### 【 0 2 2 4 】

また、上述した実施形態では、図 3 0 に示す発注者端末装置 2 1 1 の暗号化部 2 6 3 において、記憶部 2 6 5 から読み出した所定の暗号鍵を用いて、発注情報

a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、記憶部 2 6 5 から読み出した装置 ID 情報 ID<sub>M</sub> との全体に対してを暗号化を行う場合を例示したが、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 と、記憶部 2 6 5 から読み出した装置 ID 情報 ID<sub>M</sub> とのそれぞれについて個別に暗号化を行ってもよい。

【 0 2 2 5 】

### 第 9 実施形態

図 3 4 は、本実施形態のトランザクション認証システム 4 0 1 の全体構成図である。

図 3 4 に示すように、トランザクション認証システム 4 0 1 では、例えば、発注者 3 1 の発注者端末装置 4 1 1 と、受注者 3 3 の受注者端末装置 4 1 5 と、ネットワーク銀行 4 4 0 の認証装置 4 5 0 と、認証履歴を格納する認証履歴格納装置 1 4 とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者 3 1 と受注者 3 3 との間のトランザクション（取引）の正当性を認証装置 4 5 0 で認証する。

なお、当該ネットワークに接続されている発注者端末装置 4 1 1 および受注者端末装置 4 1 5 の数は任意である。

【 0 2 2 6 】

本実施形態では、認証装置 4 5 0 が第 1 5 の発明の通信装置、並びに第 1 6 および第 1 7 の発明の第 1 の通信装置に対応し、受注者端末装置 4 1 5 あるいは不正者端末装置 4 5 6 が第 1 6 および第 1 7 の発明の第 2 の通信装置に対応している。

【 0 2 2 7 】

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 4 4 0 との間で認証を行うことに関する契約が成されている。また、発注者 3 1 と引き落とし銀行 4 4 2 との間では、例えば、ネットワーク銀行 4 4 0 によって認証された取引に関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 4 4 0 と保険会社 4 4 3 との間では、ネットワーク銀行 4 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

## 【0228】

以下、トランザクション認証システム401を構成する各装置について説明する。

## 【発注者端末装置411】

図35に示すように、発注者端末装置411は、例えば、発注者31の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部461、送信部462、暗号化部463、復号部464、記憶部465、制御部466および署名検証部467を有する。

なお、発注者端末装置411は、例えば、発注者31が使用する際に、発注者31の指紋等の身体的特徴から得られる情報と、予め記憶部465に予め記憶してある身体的特徴を示す情報とを比較することで、発注者31が正当な利用者であることを認証する生体認証部を有していてもよい。

## 【0229】

ここで、受信部461が第16の発明の第2の受信手段に対応し、送信部462が第16の発明の第2の送信手段に対応している。

## 【0230】

受信部461は、ネットワークを介して認証装置450から情報あるいは要求を受信する。

送信部462は、ネットワークを介して認証装置450に情報あるいは要求を送信する。

また、受信部461および送信部462は、受注者33が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部463は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部464は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部465は、発注者31が作成した秘密鍵 $K_{31,S}$ などを格納する。

署名検証部467は、例えば、認証装置450が作成した署名情報を、ネットワーク銀行440の公開鍵 $K_{40,P}$ を用いて検証する。

制御部 4 6 6 は、発注者端末装置 4 1 1 内の各構成要素の処理を統括的に制御する。

#### 【 0 2 3 1 】

制御部 4 6 6 は、例えば、発注者 3 1 による操作に応じて、発注情報 a 1 と、個人キー情報 k 1（本発明の利用者を識別するための個人識別情報）と、個人 ID 情報 ID 1（本発明の個人識別情報）との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求 Inf 1 を生成する。

ここで、個人キー情報 k 1 および個人 ID 情報 ID 1 は、発注者 3 1 がネットワーク銀行 4 4 0 に自らを登録したときに、当該発注者 3 1 に割り当てられた固有の識別子である。例えば、個人キー情報 k 1 は、ネットワーク銀行 4 4 0 と契約した契約者（発注者 3 1）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 ID 1 は、発注者 3 1 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、制御部 4 6 6 は、例えば、認証要求 Inf 1 を認証装置 4 5 0 に送信した後に、認証装置 4 5 0 から認証応答 Inf 4 を受信したときに、認証応答 Inf 4 に含まれる認証結果を所定の表示装置や音声出力装置を介して出力する制御を行なう。

#### 【 0 2 3 2 】

##### 〔受注者端末装置 4 1 5〕

図 3 6 に示すように、受注者端末装置 4 1 5 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 3 3 が使用するサーバ装置であり、受信部 4 7 1、送信部 4 7 2、暗号化部 4 7 3、復号部 4 7 4、記憶部 4 7 5、制御部 4 7 6 および署名検証部 4 7 7 を有する。

受信部 4 7 1 は、ネットワークを介して認証装置 4 5 0 から情報あるいは要求を受信する。

送信部 4 7 2 は、ネットワークを介して認証装置 4 5 0 に情報あるいは要求を送信する。

また、受信部 4 7 1 および送信部 4 7 2 は、発注者端末装置 4 1 1 からのアク

セスに応じて、例えば、記憶部 4 7 5 から読み出した受注者 3 3 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 4 1 1 に送信する。

暗号化部 4 7 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 4 7 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 4 7 5 は、受注者 3 3 が作成した秘密鍵  $K_{33,S}$  などを格納する。

制御部 4 7 6 は、受注者端末装置 4 1 5 内の各構成要素の処理を統括的に制御する。

署名検証部 4 7 7 は、例えば、ネットワーク銀行 4 4 0 の公開鍵  $K_{40,P}$  を用いて、認証装置 4 5 0 が作成した署名情報の検証を行う。

### 【 0 2 3 3 】

#### 〔 認証装置 4 5 0 〕

図 3 7 に示すように、認証装置 4 5 0 は、受信部 4 8 1、送信部 4 8 2、暗号化部 4 8 3、復号部 4 8 4、記憶部 4 8 5、制御部 4 8 6、署名作成部 4 8 7 および課金処理部 4 8 8 を有する。

### 【 0 2 3 4 】

ここで、受信部 4 8 1 が、第 1 5 の発明の受信手段、並びに第 1 6 の発明の第 1 の受信手段に対応している。送信部 4 8 2 が、第 1 5 の発明の送信手段、並びに第 1 6 の発明の第 1 の送信手段に対応している。記憶部 4 8 5 が、第 1 5 の発明および第 1 6 の発明の記憶手段に対応している。制御部 4 8 6 が、第 1 5 の発明および第 1 6 の発明の処理手段に対応している。

### 【 0 2 3 5 】

受信部 4 8 1 は、ネットワークを介して発注者端末装置 4 1 1 および受注者端末装置 4 1 5 から情報あるいは要求を受信する。

送信部 4 8 2 は、ネットワークを介して発注者端末装置 4 1 1 および受注者端末装置 4 1 5 に情報あるいは要求を送信する。

暗号化部 4 8 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 4 8 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 4 8 5 は、発注者 3 1 がネットワーク銀行 4 4 0 と契約したときに、発注者 3 1 の個人キー情報  $k_1$  と、個人 ID 情報  $ID_1$  と、発注者 3 1 のネットワ

ーク ID\_N (本発明の送信先の情報) との対応表を図 3 7 に示す認証装置 4 5 0 の記憶部 4 8 5 に記憶する。

ここで、ネットワーク ID\_N は、発注者 3 1 がネットワーク銀行 4 4 0 にオンラインで登録した、当該ネットワークのユーザである発注者 3 1 をネットワーク内で一意に識別するための識別子である。

また、記憶部 4 8 5 は、例えば、発注者 3 1 および受注者 3 3 がネットワーク銀行 4 4 0 と契約をしたときに、発注者 3 1 が作成した秘密鍵  $K_{31,S}$  に対応する公開鍵  $K_{31,P}$ 、並びに受注者 3 3 が作成した秘密鍵  $K_{33,S}$  に対応する公開鍵  $K_{33,P}$  などを格納する。

制御部 4 8 6 は、認証装置 4 5 0 内の各構成要素の処理を統括的に制御する。

署名作成部 4 8 7 は、ネットワーク銀行 4 4 0 の秘密鍵  $K_{40,S}$  を用いて署名情報の作成を行う。

課金処理部 4 8 8 は、発注者 3 1 による取引に関する認証に対しての課金処理を行う。

認証装置 4 5 0 の各構成要素の詳細な処理については、後述する動作例で記載する。

#### 【0 2 3 6】

以下、トランザクション認証システム 4 0 1 の動作例を説明する。

当該動作例を開始する前提として、発注者 3 1 とネットワーク銀行 4 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 4 0 は、発注者 3 1 に対して、個人キー情報  $k_1$  および個人 ID 情報 ID 1 を発行している。

また、発注者 3 1 は、ネットワーク内で当該発注者 3 1 を識別するネットワーク ID\_N を、秘密が保持される環境、例えばオフラインでネットワーク銀行 4 4 0 に登録している。

ネットワーク銀行 4 4 0 は、個人キー情報  $k_1$  と、個人 ID 情報 ID 1 と、発注者 3 1 のネットワーク ID\_N との対応表を図 3 7 に示す認証装置 4 5 0 の記憶部 4 8 5 に記憶している。

#### 【0 2 3 7】

また、ネットワーク銀行 4 4 0 は、自らの秘密鍵  $K_{40,S}$  を図 3 7 に示す認証装



置 4 5 0 の記憶部 4 8 5 に記憶すると共に、当該秘密鍵  $K_{40,S}$  に対応する公開鍵  $K_{40,P}$  を発注者端末装置 4 1 1 および受注者端末装置 4 1 5 に送信する。発注者端末装置 4 1 1 は、公開鍵  $K_{40,P}$  を図 3 5 に示す記憶部 4 6 5 に記憶する。受注者端末装置 4 1 5 は、公開鍵  $K_{40,P}$  を図 3 6 に示す記憶部 4 7 5 に記憶する。

## 【 0 2 3 8 】

また、受注者 3 3 とネットワーク銀行 4 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 4 0 は、受注者 3 3 に対して、個人キー情報 Z および個人 ID 情報 ID 2 を発行する。ネットワーク銀行 4 4 0 は、個人キー情報 Z および個人 ID 情報 ID 2 の対応表を図 3 7 に示す認証装置 4 5 0 の記憶部 4 8 5 に記憶する。

## 【 0 2 3 9 】

以下、発注者 3 1 が、認証装置 4 5 0 に認証要求を行なった場合のトランザクション認証システム 4 0 1 の動作を説明する。

図 3 8 は、トランザクション認証システム 4 0 1 の当該動作を説明するための図である。

## ステップ S T 4 1 :

図 3 4 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、発注者 3 1 の個人キー情報 k 1 と、発注者 3 1 の個人 ID 情報 ID 1 とを、図示しない操作手段を操作して発注者端末装置 4 1 1 に入力する。なお、発注情報 a 1 には、受注者 3 3 を特定する情報が含まれている。

次に、図 3 5 に示す発注者端末装置 4 1 1 の暗号化部 4 6 3 は、記憶部 4 6 5 から読み出したネットワーク銀行 4 4 0 の公開鍵  $K_{40,P}$  を用いて、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 との全体に対して暗号化を行い、当該暗号化した情報を格納した認証要求 Inf 1 (本発明の要求) を、送信部 4 6 2 からネットワークを介して、図 3 4 に示すネットワーク銀行 4 4 0 の認証装置 4 5 0 に送信する。

## 【 0 2 4 0 】

## ステップ S T 4 2 :

図 3 7 に示す認証装置 4 5 0 は、発注者端末装置 4 1 1 からの認証要求  $I n f 1$  を受信部 4 8 1 が受信すると、記憶部 4 8 5 からネットワーク銀行 4 4 0 の秘密鍵  $K_{40,S}$  を読み出し、復号部 4 8 4 において、当該秘密鍵  $K_{40,S}$  を用いて認証要求  $I n f 1$  を復号する。

次に、認証装置 4 5 0 は、制御部 4 8 6 の制御に基づいて、上記復号した認証要求  $I n f 1$  から個人キー情報  $k 1$  を削除した情報  $I n f 1'$  について、記憶部 4 8 5 から読み出した自らの秘密鍵  $K_{40,S}$  を用いて署名情報  $A u 1$  を作成する。

次に、認証装置 4 5 0 は、情報  $I n f 1'$  および署名情報  $A u 1$  を格納した要求  $I n f 2$  を生成する。

次に、暗号化部 4 8 3 は、図 3 7 に示す記憶部 4 8 5 から読み出した受注者 3 3 の公開鍵  $K_{33,P}$  を用いて、上記生成した要求  $I n f 2$  を暗号化した後に、送信部 4 8 2 から、ネットワークを介して受注者端末装置 4 1 5 に送信する。

#### 【 0 2 4 1 】

##### ステップ S T 4 3 :

受注者端末装置 4 1 5 の復号部 4 7 4 は、認証装置 4 5 0 からの要求  $I n f 2$  を受信部 4 7 1 が受信すると、記憶部 4 7 5 から読み出した自らの秘密鍵  $K_{33,S}$  を用いて、要求  $I n f 2$  を復号する。

次に、受注者端末装置 4 1 5 の署名検証部 4 7 7 は、上記復号した要求  $I n f 2$  に格納された署名情報  $A u 1$  を、記憶部 4 7 5 から読み出した認証装置 4 5 0 の公開鍵  $K_{40,P}$  を用いて検証する。

#### 【 0 2 4 2 】

受注者端末装置 4 1 5 の制御部 4 7 6 は、署名検証部が上記検証の結果、署名情報  $A u 1$  の正当性が認証されると、要求  $I n f 2$  に格納された情報  $I n f 1'$  を図 3 6 に示す記憶部 4 7 5 に記憶する。受注者 3 3 は、情報  $I n f 1'$  内の発注情報  $a 1$  に基づいて、発注者 3 1 への商品等の発送予定などを示す受注確認情報  $c 1$  を生成する。

次に、制御部 4 7 6 は、要求  $I n f 2$ 、受注確認情報  $c 1$  および自らの個人キー情報  $Z$  を格納した応答  $I n f 3$  を生成する。

次に、受注者端末装置 4 1 5 の送信部 4 7 2 は、上記生成した応答 I n f 3 を、記憶部 4 7 5 から読み出したネットワーク銀行 4 4 0 の公開鍵  $K_{40,P}$  を用いて暗号化部 4 7 3 で暗号化した後に、送信部 4 7 2 から、ネットワークを介して認証装置 4 5 0 に送信する。

受注者 3 3 は、例えば、要求 I n f 2 に格納された情報 I n f 1' 内の発注情報 a 1 に基づいて、発注者 3 1 が発注した商品等を発注者 3 1 に発送したり、発注者 3 1 が注文したサービスを発注者 3 1 に提供する。

### 【 0 2 4 3 】

ステップ S T 4 4 :

認証装置 4 5 0 の復号部 4 8 4 は、受注者端末装置 4 1 5 からの応答 I n f 3 を受信部 4 8 1 が受信すると、記憶部 4 8 5 から読み出した自らの秘密鍵  $K_{40,S}$  を用いて、I n f 3 を復号し、要求 I n f 1 に格納された発注情報 a 1 と、当該復号された I n f 3 に格納された受注者 3 3 の個人キー情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 4 8 5 に格納する。当該履歴情報は、ネットワーク銀行 4 4 0 が、発注者 3 1 に対して決済を行う際に用いられる。

また、認証装置 4 5 0 の署名作成部 4 8 7 は、ステップ S T 4 3 で受信した応答 I n f 3 について、自らの秘密鍵  $K_{40,S}$  を用いて署名情報 A u 2 を作成する。

次に、認証装置 4 5 0 の制御部 4 8 6 は、応答 I n f 3 および署名情報 A u 2 を格納した認証応答 I n f 4 を作成する。

次に、認証装置 4 5 0 の暗号化部 4 8 3 は、上記作成し認証した応答 I n f 4 を、公開鍵  $K_{31,P}$  を用いて暗号化した後に、個人 I D 情報 I D 1 に対応する記憶部 4 8 5 から読み出した発注者 3 1 のネットワーク I D \_ N に基づいて送信先を特定して、送信部 4 8 2 からネットワークを介して発注者端末装置 4 1 1 に送信する。

### 【 0 2 4 4 】

発注者端末装置 4 1 1 では、受信した認証応答 I n f 4 を、図 3 5 に示す記憶部 4 6 5 から読み出した発注者 3 1 の秘密鍵  $K_{31,S}$  を用いて復号部 4 6 4 で復号する。

次に、発注者端末装置 4 1 1 の署名検証部 4 6 6 は、当該復号した認証応答 I

nf 4 に格納された署名情報 Au 2 を、記憶部 465 から読み出したネットワーク銀行 440 の公開鍵  $K_{40,p}$  を用いて検証する。

当該検証によってその正当性が確認されると、制御部 466 は、認証応答 Inf 4 に格納されている発注情報 a 1 や取り引きの内容を示す情報に応じた出力を、発注者端末装置 411 の図示しないディスプレイやスピーカから出力する。

#### 【0245】

以下、発注者 31 の個人 ID 1 および個人キー k 1 を不正に取得した図 34 に示す不正者 55 が自らの端末装置である不正者端末装置 456 を用いて、認証装置 450 に認証要求を送信した場合のトランザクション認証システム 401 の動作を説明する。

ここで、不正者端末装置 456 の構成は、例えば、図 35 に示す発注者端末装置 411 と同じである。

図 39 は、トランザクション認証システム 401 の当該動作を説明するための図である。

#### ステップ ST 51 :

図 34 に示す不正者 55 は、受注者 33 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、不正に取得した発注者 31 の個人キー情報 k 1 と、不正に取得した発注者 31 の個人 ID 情報 ID 1 とを、図示しない操作手段を操作して不正者端末装置 456 に入力する。

次に、不正者端末装置 456 の図 35 に示す暗号化部 463 は、記憶部 465 から読み出したネットワーク銀行 440 の公開鍵  $K_{40,p}$  を用いて、発注情報 a 1 と、個人キー情報 k 1 と、個人 ID 情報 ID 1 との全体に対して暗号化を行い、当該暗号化した情報を格納した認証要求 Inf 1 を、送信部 462 からネットワークを介して、図 34 に示すネットワーク銀行 440 の認証装置 450 に送信する。

#### 【0246】

#### ステップ ST 52 :

図 37 に示す認証装置 450 は、不正者端末装置 456 からの認証要求 Inf 1 を受信部 481 が受信すると、当該認証要求 Inf 1 について、前述したステ

ップST42と同様の処理を行なう。

【0247】

ステップST53：

ステップST53の処理は、前述したステップST43の処理と同じである。

【0248】

ステップST54：

ステップST54の処理は、前述したステップST44の処理と同じである。

すなわち、不正者55が不正者端末装置456を用いて、認証要求Inf1を認証装置450に送信した場合でも、その応答である認証応答Inf4は、認証装置450の記憶部485に記憶されている発注者31のネットワークID\_Nに基づいて、発注者端末装置411に送信される。

これにより、発注者31は、受信した認証応答Inf4に基づいて、自らが個人ID情報ID1を用いた不正な認証要求が行なわれたことを知ることができ、その旨をネットワーク銀行440などに通知する。

【0249】

以上説明したように、トランザクション認証システム401によれば、認証装置450は、発注者31がネットワーク銀行440にオフラインで登録したネットワークID\_Nによって指定された送信先に、認証応答Inf4を送信するため、例えば、発注者31の個人情報ID1を不正に取得した者が当該個人情報ID1を用いて認証装置450に認証要求を行なった場合に、認証装置450に登録されたネットワークID\_Nに基づいて認証装置450から発注者端末装置411に送信された認証応答Inf4によって、発注者31は自らの個人情報ID1を用いた不正な取り引きが行なわれることを知ることができる。

そのため、トランザクション認証システム401によれば、他人の個人情報を用いた不正な取り引きを効果的に抑制できる。

【0250】

上述したように、トランザクション認証システム401によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させ

ることが可能になる。

#### 【0251】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の処理手段が行う処理として認証処理を例示したが、その他、課金処理などの処理を行う場合にも本発明は適用可能である。

#### 【0252】

また、上述した実施形態では、ネットワーク銀行440が、認証装置450を用いて、トランザクション（取引）の認証業務を行う場合を例示したが、ネットワーク銀行440とは別の機関が、認証装置450を用いてトランザクションの認証業務を行うようにしてもよい。

#### 【0253】

##### 第10実施形態

図40は、本実施形態のトランザクション認証システム501の全体構成図である。

図40に示すように、トランザクション認証システム501では、例えば、発注者31の発注者端末装置511と、受注者33の受注者端末装置515と、ネットワーク銀行540の認証装置550と、認証履歴を格納する認証履歴格納装置14とが、インターネットなどの外部ネットワーク（通信網）509を介して接続されており、発注者31と受注者33との間のトランザクション（取引）の正当性を認証装置550で認証する。

なお、当該外部ネットワーク509に接続されているホームネットワークシステム（発注者端末システム）10および受注者端末装置515の数は任意である。

#### 【0254】

本実施形態は、第18～20の発明に対応した実施形態である。

本実施形態では、ホームネットワークシステム510が本発明の通信制御装置に対応し、端末装置511<sub>1</sub>～511<sub>4</sub>が本発明の第1の通信装置に対応し、認証装置550が本発明の第2の通信装置に対応している。

## 【 0 2 5 5 】

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 5 4 0 との間で認証を行うことに関しての契約が成されている。また、発注者 3 1 と引き落とし銀行 5 4 2 との間では、例えば、ネットワーク銀行 5 4 0 によって認証された取引引きに関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 5 4 0 と保険会社 5 4 3 との間では、ネットワーク銀行 5 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

## 【 0 2 5 6 】

以下、トランザクション認証システム 5 0 1 を構成する各装置について説明する。

## 〔ホームネットワークシステム 5 1 0〕

図 4 0 および図 4 1 に示すように、ホームネットワークシステム 5 1 0 は、発注者 3 1 の各家庭などに構築されており、ホームネットワークシステム 5 1 0 のホームゲートウェイ 5 1 2 が、図 4 0 に示す受注者端末装置 5 1 5 および認証装置 5 5 0 が接続される外部ネットワーク 5 0 9 に有線あるいは無線で接続されている。

また、ホームゲートウェイ 5 1 2 には、例えば、家庭内の内部ネットワーク 1 3 を介して、端末装置 5 1 1<sub>1</sub> , 1 1<sub>2</sub> , 1 1<sub>3</sub> , 1 1<sub>4</sub> が有線あるいは無線で接続される。

端末装置 5 1 1<sub>1</sub> ~ 1 1<sub>4</sub> は、例えば、デジタルテレビ受信装置、パーソナルコンピュータ、電話機およびゲーム機などである。

端末装置 5 1 1<sub>1</sub> ~ 1 1<sub>4</sub> の各々には、例えば製造元で当該端末装置を識別するための装置 ID 情報が割り当てられており、当該装置 ID 情報が各端末装置の内部メモリに記憶されている。例えば、端末装置 5 1 1<sub>1</sub> には装置 ID 情報 ID<sub>M1</sub> が割り当てられ、端末装置 5 1 1<sub>2</sub> には装置 ID 情報 ID<sub>M2</sub> が割り当てられ、端末装置 5 1 1<sub>3</sub> には装置 ID 情報 ID<sub>M3</sub> が割り当てられ、端末装置 5 1 1<sub>4</sub> には装置 ID 情報 ID<sub>M4</sub> が割り当てられている。

## 【 0 2 5 7 】

図42は、ホームゲートウェイ512の構成図である。

ホームゲートウェイ512は、例えば、外部ネットワークI/F561、内部ネットワークI/F562、暗号化部563、復号部564、記憶部565、制御部566および署名検証部567を有する。

ここで、外部ネットワークI/F561および内部ネットワークI/F562が、第18の発明の送信手段および受信手段、並びに第19の発明の第1の送信手段および第2の受信手段に対応している。また、記憶部565が、第18の発明の記憶手段および第19の発明の第1の記憶手段に対応している。また、制御部566が第18の発明および第19の発明の制御手段に対応している。

#### 【0258】

外部ネットワークI/F561は、外部ネットワーク509を介して認証装置550との間で、情報あるいは要求の送受信を行なう。

内部ネットワークI/F562は、内部ネットワーク13を介して端末装置511<sub>1</sub>～511<sub>4</sub>との間で、情報あるいは要求の送受信を行なう。

暗号化部563は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部564は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部565は、例えば、ホームゲートウェイ512の電源が投入されたときに電源がオンになっている端末装置511<sub>1</sub>～511<sub>4</sub>から内部ネットワーク13を介して受信した装置ID情報ID<sub>M1</sub>～ID<sub>M4</sub>を記憶している。

また、記憶部565は、発注者31が作成した秘密鍵K<sub>31,S</sub>などを格納する。

署名検証部567は、例えば、認証装置550が作成した署名情報を、ネットワーク銀行540の公開鍵K<sub>40,P</sub>を用いて検証する。

制御部566は、発注者端末装置511内の各構成要素の処理を統括的に制御する。

制御部566は、ホームゲートウェイ512を介した端末装置511<sub>1</sub>～511<sub>4</sub>と認証装置550との間の通信の履歴を示す履歴情報を生成し、これを記憶部565に記憶する。

そのため、記憶部565に記憶された履歴情報にアクセスを行うだけで、家庭内に設けられた端末装置511<sub>1</sub>～511<sub>4</sub>を用いた通信の履歴を簡単に知るこ



とができ、管理が容易になる。

【0259】

また、制御部566は、例えば、待機状態（スタンバイ状態）になっている端末装置511<sub>1</sub>～511<sub>4</sub>に対してのアクセスを、外部ネットワーク509を介して受けた場合に、対応する端末装置511<sub>1</sub>～511<sub>4</sub>が動作状態になるように制御する。

【0260】

制御部566は、例えば、発注者31による操作に応じて端末装置511<sub>1</sub>～511<sub>4</sub>から内部ネットワークI/F562が受信した、発注情報a1と、個人キー情報k1と（本発明の個人識別情報）、個人ID情報ID1（本発明の個人識別情報）と、装置ID情報ID<sub>M1</sub>～ID<sub>M4</sub>（本発明の装置識別情報）との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求Inf1を生成する。

また、制御部566は、例えば、認証要求Inf1を認証装置550に送信した後に、認証装置550から認証応答Inf4を受信したときに、認証応答Inf4に含まれる認証要求の送信元の装置を示す装置ID情報と、記憶部565から読み出した装置ID情報ID<sub>M1</sub>～ID<sub>M4</sub>の何れかとが一致するか否かを検出し、一致している場合には、正当な取り引きが行われていると判断し、不一致の場合には、不正な取り引きが行われたと判断して、その旨を受注者端末装置515および認証装置550の少なくとも一方に通知する。

【0261】

〔受注者端末装置515〕

図43に示すように、受注者端末装置515は、サイバーモール(Cyber Mall)などに店舗を出している受注者33が使用するサーバ装置であり、受信部571、送信部572、暗号化部573、復号部574、記憶部575、制御部576および署名検証部577を有する。

受信部571は、外部ネットワーク509を介して認証装置550から情報あるいは要求を受信する。

送信部572は、外部ネットワーク509を介して認証装置550に情報ある

いは要求を送信する。

また、受信部 571 および送信部 572 は、発注者端末装置 511 からのアクセスに応じて、例えば、記憶部 575 から読み出した受注者 33 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 511 に送信する。

暗号化部 573 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 574 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 575 は、受注者 33 が作成した秘密鍵  $K_{33,S}$  などを格納する。

制御部 576 は、受注者端末装置 515 内の各構成要素の処理を統括的に制御する。

署名検証部 577 は、例えば、ネットワーク銀行 540 の公開鍵  $K_{40,P}$  を用いて、認証装置 550 が作成した署名情報の検証を行う。

【0262】

〔認証装置 550〕

図 44 に示すように、認証装置 550 は、受信部 581、送信部 582、暗号化部 583、復号部 584、記憶部 585、制御部 586、署名作成部 587 および課金処理部 588 を有する。

【0263】

ここで、受信部 581 が第 19 の発明の第 2 の受信手段に対応し、送信部 582 が第 19 の発明の第 2 の送信手段に対応し、記憶部 585 が第 19 の発明の第 2 の記憶手段に対応し、制御部 586 が第 19 の発明の処理手段に対応している。

【0264】

受信部 581 は、外部ネットワーク 509 を介してホームゲートウェイ 512 および受注者端末装置 515 から情報あるいは要求を受信する。

送信部 582 は、外部ネットワーク 509 を介してホームゲートウェイ 512 および受注者端末装置 515 に情報あるいは要求を送信する。

暗号化部 583 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 584 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 585 は、発注者 31 がネットワーク銀行 540 と契約したときに、発

注者 31 の個人キー情報  $k_1$  と、個人 ID 情報  $ID_1$  と、ホームゲートウェイ 512 のアドレスとの対応表を記憶する。また、記憶部 585 は、例えば、発注者 31 および受注者 33 がネットワーク銀行 540 と契約をしたときに、発注者 31 が作成した秘密鍵  $K_{31,S}$  に対応する公開鍵  $K_{31,P}$ 、並びに受注者 33 が作成した秘密鍵  $K_{33,S}$  に対応する公開鍵  $K_{33,P}$  などを格納する。

制御部 586 は、認証装置 550 内の各構成要素の処理を統括的に制御する。

署名作成部 587 は、ネットワーク銀行 540 の秘密鍵  $K_{40,S}$  を用いて署名情報の作成を行う。

課金処理部 588 は、発注者 31 による取引に関する認証に対しての課金処理を行う。

認証装置 550 の各構成要素の詳細な処理については、後述する動作例で記載する。

#### 【0265】

以下、トランザクション認証システム 501 の動作例を説明する。

当該動作例では、図 40 に示す発注者 31 が図 41 に示す端末装置 511<sub>1</sub> を操作して、受注者 33 が提供する商品またはサービスの発注を行なう場合を説明する。

なお、当該動作例を開始する前提として、以下の手続および処理が行なわれている。

すなわち、発注者 31 とネットワーク銀行 540 との間で所定の契約が結ばれ、ネットワーク銀行 540 は、発注者 31 に対して、個人キー情報  $k_1$  および個人 ID 情報  $ID_1$  を発行する。

ネットワーク銀行 540 は、個人キー情報  $k_1$  と、個人 ID 情報  $ID_1$  と、ホームゲートウェイ 512 のアドレスとの対応表を図 44 に示す認証装置 550 の記憶部 585 に記憶する。ここで、個人キー情報  $k_1$  は、例えば、ネットワーク銀行 540 と契約した契約者（発注者 31）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報  $ID_1$  は、発注者 31 の銀行口座番号などの課金に係わる情報を示す識別子である。

#### 【0266】

また、ネットワーク銀行540は、自らの秘密鍵 $K_{40,S}$ を図44に示す認証装置550の記憶部585に記憶すると共に、当該秘密鍵 $K_{40,S}$ に対応する公開鍵 $K_{40,P}$ をホームゲートウェイ512および受注者端末装置515に送信する。ホームゲートウェイ512は、公開鍵 $K_{40,P}$ を図42に示す記憶部565に記憶する。受注者端末装置515は、公開鍵 $K_{40,P}$ を図43に示す記憶部575に記憶する。

#### 【0267】

また、受注者33とネットワーク銀行540との間で所定の契約が結ばれ、ネットワーク銀行540は、受注者33に対して、個人キー情報Zおよび個人ID情報ID2を発行する。ネットワーク銀行540は、個人キー情報Zおよび個人ID情報ID2の対応表を図44に示す認証装置550の記憶部585に記憶する。

#### 【0268】

また、ホームゲートウェイ512の電源が投入されたときに電源がオンになっている端末装置511<sub>1</sub>～511<sub>4</sub>から内部ネットワーク13を介してホームゲートウェイ512が受信した装置ID情報ID<sub>M1</sub>～ID<sub>M4</sub>が、図42に示す記憶部565に記憶される。

#### 【0269】

図45は、トランザクション認証システム501の動作例を説明するための図である。

#### ステップST61：

図40に示す発注者31は、例えばネットワーク上の商店である受注者33に商品を発注する場合に、発注する商品名および数量などを示す発注情報a1と、発注者31の個人キー情報k1と、発注者31の個人ID情報ID1とを、図示しない操作手段を操作して端末装置511<sub>1</sub>に入力する。なお、発注情報a1には、受注者33を特定する情報が含まれている。

端末装置511<sub>1</sub>は、当該入力された発注情報a1と、発注者31の個人キー情報k1と、発注者31の個人ID情報ID1と、内部メモリから読み出した装置ID情報ID<sub>M1</sub>とを、内部ネットワーク13を介して、ホームゲートウェイ5

12に送信する。

【0270】

ステップST62:

図42に示すホームゲートウェイ512は、発注情報a1と、個人キー情報k1と、個人ID情報ID1と、装置ID情報ID<sub>M1</sub>とを内部ネットワークI/F562で受信し、これらの全体に対して暗号化部563で暗号化を行う。

ホームゲートウェイ512は、当該暗号化した情報を格納した認証要求Inf1（本発明の要求）を、図42に示す外部ネットワークI/F561から外部ネットワーク509を介して、図40に示すネットワーク銀行540の認証装置550に送信する。

【0271】

ステップST63:

図44に示す認証装置550は、ホームゲートウェイ512からの認証要求Inf1を受信部581が受信すると、記憶部585からネットワーク銀行540の秘密鍵K<sub>40,S</sub>を読み出し、復号部584において、当該秘密鍵K<sub>40,S</sub>を用いて認証要求Inf1を復号する。

次に、認証装置550は、制御部586の制御に基づいて、上記復号した認証要求Inf1から個人キー情報k1を削除した情報Inf1' について、記憶部585から読み出した自らの秘密鍵K<sub>40,S</sub>を用いて署名情報Au1を作成する。

次に、認証装置550は、情報Inf1' および署名情報Au1を格納した要求Inf2を生成する。

次に、暗号化部583は、図44に示す記憶部585から読み出した受注者33の公開鍵K<sub>33,P</sub>を用いて、上記生成した要求Inf2を暗号化した後に、送信部582から、外部ネットワーク509を介して受注者端末装置515に送信する。

【0272】

ステップST64:

受注者端末装置515の復号部574は、認証装置550からの要求Inf2

を受信部 571 が受信すると、記憶部 575 から読み出した自らの秘密鍵  $K_{33,S}$  を用いて、要求 Inf 2 を復号する。

次に、受注者端末装置 515 の署名検証部 577 は、上記復号した要求 Inf 2 に格納された署名情報 Au 1 を、記憶部 575 から読み出した認証装置 550 の公開鍵  $K_{40,P}$  を用いて検証する。

### 【0273】

受注者端末装置 515 の制御部 576 は、署名検証部が上記検証の結果、署名情報 Au 1 の正当性が認証されると、要求 Inf 2 に格納された情報 Inf 1' を図 43 に示す記憶部 575 に記憶する。受注者 33 は、情報 Inf 1' 内の発注情報 a 1 に基づいて、発注者 31 への商品等の発送予定などを示す受注確認情報 c 1 を生成する。

次に、制御部 576 は、要求 Inf 2、受注確認情報 c 1 および自らの個人キー情報 Z を格納した応答 Inf 3 を生成する。

次に、受注者端末装置 515 の送信部 572 は、上記生成した応答 Inf 3 を、記憶部 575 から読み出したネットワーク銀行 540 の公開鍵  $K_{40,P}$  を用いて暗号化部 573 で暗号化した後に、送信部 572 から、外部ネットワーク 509 を介して認証装置 550 に送信する。

受注者 33 は、例えば、要求 Inf 2 に格納された情報 Inf 1' 内の発注情報 a 1 に基づいて、発注者 31 が発注した商品等を発注者 31 に発送したり、発注者 31 が注文したサービスを発注者 31 に提供する。

### 【0274】

#### ステップ ST 65 :

認証装置 550 の復号部 584 は、受注者端末装置 515 からの応答 Inf 3 を受信部 581 が受信すると、記憶部 585 から読み出した自らの秘密鍵  $K_{40,S}$  を用いて、Inf 3 を復号し、要求 Inf 1 に格納された発注情報 a 1 と、当該復号された Inf 3 に格納された受注者 33 の個人キー情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 585 に格納する。当該履歴情報は、ネットワーク銀行 540 が、発注者 31 に対して決済を行う際に用いられる。

また、認証装置 550 の署名作成部 587 は、ステップ ST 64 で受信した応

答 I n f 3 について、自らの秘密鍵  $K_{40,S}$  を用いて署名情報 A u 2 を作成する。

次に、認証装置 5 5 0 の制御部 5 8 6 は、応答 I n f 3 および署名情報 A u 2 を格納した認証応答 I n f 4 を作成する。

次に、認証装置 5 5 0 の暗号化部 5 8 3 は、上記作成した認証応答 I n f 4 を、記憶部 5 8 5 から読み出した発注者 3 1 の公開鍵  $K_{31,P}$  を用いて暗号化する。

そして、図 4 4 に示す記憶部 5 8 5 に個人 I D 情報 I D 1 と対応して記憶されているホームゲートウェイ 5 1 2 のアドレスを用いて、送信部 5 8 2 から外部ネットワーク 5 0 9 を介してホームゲートウェイ 5 1 2 に当該暗号化した応答 I n f 4 を送信する。

ホームゲートウェイ 5 1 2 では、受信した認証応答 I n f 4 を、図 4 2 示す記憶部 5 6 5 から読み出した発注者 3 1 の秘密鍵  $K_{31,S}$  を用いて復号部 5 6 4 で復号する。

次に、ホームゲートウェイ 5 1 2 の署名検証部 5 6 6 は、当該復号した認証応答 I n f 4 に格納された署名情報 A u 2 を、記憶部 5 6 5 から読み出したネットワーク銀行 5 4 0 の公開鍵  $K_{40,P}$  を用いて検証すると共に、I n f 4 内の発注情報 a 1 内に記述された装置 I D 情報 I D<sub>M1</sub> が図 4 2 に示す記憶部 5 6 5 に記憶されている装置 I D 情報 I D<sub>M1</sub> ~ I D<sub>M4</sub> の何れかと一致するか否かを判断する。当該動作例では、一致すると判断され、発注者 3 1 と受注者 3 3 との間の当該取り引きが正当に行われたことが確認される。

#### 【 0 2 7 5 】

ステップ S T 6 6 :

ホームゲートウェイ 5 1 2 は、応答 I n f 4 に含まれる I n f 3 を、内部ネットワーク 1 3 を介して端末装置 5 1 1<sub>1</sub> に送信する。

端末装置 5 1 1<sub>1</sub> は、当該受信した I n f 3 に格納された受注確認情報 c 1 をディスプレイなどに表示する。

#### 【 0 2 7 6 】

以下、発注者 3 1 の個人 I D 1 および個人キー k 1 を不正に取得した図 4 0 に示す不正者 5 5 が自らの端末装置である不正者端末装置 5 5 6 を用いて、認証装置 5 5 0 に認証要求を送信した場合のトランザクション認証システム 5 0 1 の動

作を説明する。

図46は、トランザクション認証システム501の当該動作を説明するための図である。

ステップST71:

図40に示す不正者55は、受注者33に商品を発注する場合に、発注する商品名および数量などを示す発注情報a1と、不正に取得した発注者31の個人キー情報k1と、不正に取得した発注者31の個人ID情報ID1とを、図示しない操作手段を操作して不正者端末装置556に入力する。

不正者端末装置556は、発注情報a1と、個人キー情報k1と、個人ID情報ID1と、内部メモリから読み出した装置ID情報ID<sub>M56</sub>を暗号化し、当該暗号化した情報を格納した認証要求Inf1を、外部ネットワーク509を介して、図40に示すネットワーク銀行540の認証装置550に送信する。

図44に示す認証装置550は、不正者端末装置556からの認証要求Inf1を受信部581が受信すると、当該認証要求Inf1について、前述したステップST62と同様の処理を行なう。

【0277】

ステップST72:

ステップST72の処理は、前述したステップST63の処理と同じである。

【0278】

ステップST73:

ステップST73の処理は、前述したステップST64の処理と同じである。

【0279】

ステップST74:

ステップST74の処理は、前述したステップST65の処理と同じである。

【0280】

ステップST75:

ステップST75の処理は、前述したステップST66の処理と同じである。

【0281】

このように、トランザクション認証システム501によれば、不正者55が不



正者端末装置 556 を用いて、認証要求 Inf 1 を認証装置 550 に送信した場合でも、その応答である認証応答 Inf 4 は、認証装置 550 の記憶部 585 に個人 ID 情報 ID 1 と対応して記憶されているホームゲートウェイ 512 のアドレスに基づいて、ホームゲートウェイ 512 に送信される。

これにより、ホームゲートウェイ 512 において、認証応答 Inf 4 に含まれる装置 ID 情報 ID<sub>M56</sub> が、図 42 に示す記憶部 565 に記憶されている装置 ID 情報 ID<sub>M1</sub> ~ ID<sub>M4</sub> と一致しないと判断され、発注者 31 の個人 ID 情報 ID 1 を用いた不正な認証要求が行なわれたことを検出できる。

そのため、トランザクション認証システム 501 によれば、他人の個人 ID 情報を用いた不正な取り引きを効果的に抑制できる。

#### 【0282】

上述したように、トランザクション認証システム 501 によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取り引き者）の数を増やし、各契約者に課す会費などの費用を低額にでき、電子商取引をさらに普及させることが可能になる。

#### 【0283】

また、トランザクション認証システム 501 によれば、例えば、図 40 および図 41 に示す端末装置 511<sub>1</sub> からの要求に応じて認証要求 Inf 1 を認証装置 550 に送信した後に、端末装置 511<sub>1</sub> が故障した場合でも、当該認証要求 Inf 1 に応じた認証応答 Inf 4 に応じた処理を適切に行うことができる。

#### 【0284】

また、トランザクション認証システム 501 によれば、外部ネットワーク 509 を介した通信に伴うセキュリティに関する機能をホームゲートウェイ 512 に持たせることで、端末装置 511<sub>1</sub> ~ 11<sub>4</sub> に備えるセキュリティ機能のレベルを下げることができ、端末装置 511<sub>1</sub> ~ 11<sub>4</sub> の構成を簡単かつ安価にできる。

#### 【0285】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の第 2 の通信装置として認証処理を行

う認証装置 5 5 0 を例示したが、第 2 の通信装置が行う処理はその他、課金処理などであってもよい。

また、上述した実施形態では、ネットワーク銀行 5 4 0 が、認証装置 5 5 0 を用いて、トランザクション（取引）の認証業務を行う場合を例示したが、ネットワーク銀行 5 4 0 とは別の機関が、認証装置 5 5 0 を用いてトランザクションの認証業務を行うようにしてもよい。

#### 【 0 2 8 6 】

また、上述した実施形態では、端末装置 5 1 1<sub>1</sub> ～ 1 1<sub>4</sub> の装置 I D 情報を認証装置 5 5 0 に送信した場合を例示したが、ホームゲートウェイ 5 1 2 の装置 I D 情報を認証装置 5 5 0 に送信するようにしてもよい。

#### 【 0 2 8 7 】

##### 【発明の効果】

以上説明したように本発明によれば、ネットワークを介した電子商取引の安全性を高めことができる認証装置、処理装置、認証システムおよびその方法を提供できる。

また、本発明によれば、第 1 の取引引き者の個人キー情報が第 2 の取引引き者に提供されないようにすることで、個人キー情報を用いた不正行為を効果的に抑制する認証装置、処理装置、認証システムおよびその方法を提供できる。

#### 【 0 2 8 8 】

また、本発明によれば、不正に取得した他人の識別情報（個人 I D 情報）に基づいて不正な認証手続が行われることを回避する認証装置、処理装置、認証システムおよびその方法を提供できる。

#### 【 0 2 8 9 】

また、本発明によれば、例えば異なる認証機関と契約した複数の取引引き者間での取引引きの認証を、取引引き者の個人情報を他の認証機関に提供することなく、高い信頼性で行うことができる認証装置、認証システムおよびその方法を提供できる。

#### 【 0 2 9 0 】

また、本発明によれば、不正に取得した他人の識別情報（個人 I D 情報）に基

づいて不正な手続が行われることを回避する通信装置、通信システムおよびその方法を提供できる。

【0291】

また、本発明によれば、不正に取得した他人の識別情報（個人ID情報）に基づいて不正な認証手続が行われることを回避する通信制御装置、通信システムおよびその方法を提供できる。

また、本発明によれば、複数の通信装置を用いてネットワークを介した電子商取引などを行う場合に、当該電子商取引に必要な機能の割り当て、並びに通信履歴の管理を効率的に行うことができる通信制御装置、通信システムおよびその方法を提供できる。

【0292】

また、本発明によれば、情報を高い秘匿性を保ちながら記録媒体に記録できる情報記録方法およびその装置と、そのような形態で情報が記録された記録媒体とを提供できる。

また、本発明によれば、上述したような情報記録方法およびその装置によって記録媒体に記録された情報を適切に復元できる情報復元方法およびその装置を提供できる。

【図面の簡単な説明】

【図1】

図1は、本発明の第1実施形態に係わるトランザクション認証システムの全体構成図である。

【図2】

図2は、図1に示す発注者端末装置の機能ブロック図である。

【図3】

図3は、図1に示す認証装置の機能ブロック図である。

【図4】

図4は、図1に示す受注者端末装置の機能ブロック図である。

【図5】

図5は、図1に示すトランザクション認証システムの動作を説明するための図

である。

【図 6】

図 6 は、本発明の第 2 実施形態に係わるトランザクション認証システムの全体構成図である。

【図 7】

図 7 は、図 6 に示す発注者端末装置の機能ブロック図である。

【図 8】

図 8 は、図 6 に示す認証装置の機能ブロック図である。

【図 9】

図 9 は、図 6 に示す受注者端末装置の機能ブロック図である。

【図 10】

図 10 は、図 6 に示すトランザクション認証システムの動作を説明するための図である。

【図 11】

図 11 は、本発明の第 3 実施形態のトランザクション認証システムの全体構成図である。

【図 12】

図 12 は、図 11 に示す発注者端末装置の構成図である。

【図 13】

図 13 は、図 11 に示す受注者端末装置の構成図である。

【図 14】

図 14 は、図 11 に示す認証装置（A）の構成図である。

【図 15】

図 15 は、図 11 に示す認証装置（B）の構成図である。

【図 16】

図 16 は、図 11 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図 17】

図 17 は、本発明の第 4 実施形態の情報記録装置の構成図である。

【図 18】

図 18 は、図 17 に示す情報記録装置における処理の情報の流れを説明するための図である。

【図 19】

図 19 は、図 17 に示す情報記録装置の処理のフローチャートである。

【図 20】

図 20 は、本発明の第 5 実施形態の情報復元装置の構成図である。

【図 21】

図 21 は、図 20 に示す情報復元装置における処理の情報の流れを説明するための図である。

【図 22】

図 22 は、図 20 に示す情報復元装置の処理のフローチャートである。

【図 23】

図 23 は、本発明の第 6 実施形態の情報記録装置の構成図である。

【図 24】

図 24 は、図 23 に示す情報記録装置における処理の情報の流れを説明するための図である。

【図 25】

図 25 は、図 23 に示す情報記録装置の処理のフローチャートである。

【図 26】

図 26 は、本発明の第 7 実施形態の情報復元装置の構成図である。

【図 27】

図 27 は、図 26 に示す情報復元装置における処理の情報の流れを説明するための図である。

【図 28】

図 28 は、図 26 に示す情報復元装置の処理のフローチャートである。

【図 29】

図 29 は、本発明の第 8 実施形態に係わるトランザクション認証システムの全体構成図である。

【図 3 0】

図 3 0 は、図 2 9 に示す発注者端末装置の構成図である。

【図 3 1】

図 3 1 は、図 2 9 に示す受注者端末装置の構成図である。

【図 3 2】

図 3 2 は、図 2 9 に示す認証装置の構成図である。

【図 3 3】

図 3 3 は、図 2 9 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図 3 4】

図 3 4 は、本発明の第 9 実施形態のトランザクション認証システムの全体構成図である。

【図 3 5】

図 3 5 は、図 3 4 に示す発注者端末装置の構成図である。

【図 3 6】

図 3 6 は、図 3 4 に示す受注者端末装置の構成図である。

【図 3 7】

図 3 7 は、図 3 4 に示す認証装置の構成図である。

【図 3 8】

図 3 8 は、発注者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

【図 3 9】

図 3 9 は、不正者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

【図 4 0】

図 4 0 は、本発明の第 1 0 実施形態のトランザクション認証システムの全体構成図である。

【図 4 1】

図 4 1 は、図 4 0 に示すホームネットワークシステムを説明するための図であ

る。

【図 4 2】

図 4 2 は、図 4 1 に示すホームゲートウェイの構成図である。

【図 4 3】

図 4 3 は、図 4 0 に示す受注者端末装置の構成図である。

【図 4 4】

図 4 4 は、図 4 0 に示す認証装置の構成図である。

【図 4 5】

図 4 5 は、正当者が認証要求を出した場合の図 4 0 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【図 4 6】

図 4 6 は、不正者が認証要求を出した場合の図 4 0 に示すトランザクション認証システムの動作例を説明するための情報の流れを示す図である。

【符号の説明】

1…トランザクション認証システム、11…発注者端末装置、11a…認証要求入力部、11b…認証要求送信部、11c…認証応答受信部、11d…認証要求暗号化部、11e…認証応答復号部、12…生体認証装置、13…認証装置、13a…認証要求受信部、13b…発注者認証部、13c…要求生成部、13d…要求送信部、13e…応答受信部、13f…受注者認証部、13g…認証応答生成部、13h…認証応答暗号化部、13i…認証応答送信部、13j…要求暗号化部、13k…応答復号部、13l…認証要求復号部、14…認証履歴格納装置、15…受注者端末装置、15a…認証要求受信部、15b…要求復号部、15c…応答入力部、15d…応答生成部、15e…応答暗号化部、15f…応答送信部、

101…トランザクション認証システム、11…発注者端末装置、11a…認証要求入力部、11b…認証要求送信部、11c…認証応答受信部、11d…認証要求暗号化部、11e…認証応答復号部、12…生体認証装置、13…認証装置、113a…認証要求受信部、113b…発注者認証部、113c…要求生成部、113d…要求送信部、113e…応答受信部、113f…受注者認証部、

113g…認証応答生成部、113h…認証応答暗号化部、113i…認証応答送信部、113j…要求暗号化部、113k…応答復号部、113l…認証要求復号部、14…認証履歴格納装置、15…受注者端末装置、115a…認証要求受信部、115b…要求復号部、115c…応答入力部、115d…応答生成部、115e…応答暗号化部、115f…応答送信部

201…トランザクション認証システム、211…発注者端末装置、215…受注者端末装置、31…発注者、33…受注者、240…ネットワーク銀行、250…認証装置、261, 271, 281…受信部、262, 272, 282…送信部、263, 273, 283…暗号化部、264, 274, 284…復号部、265, 275, 285…記憶部、266, 276, 286…制御部、267, 277…署名検証部、287…署名作成部、288…課金処理部、a1…発注情報、k1…発注者31の個人キー情報k1、ID1…発注者31の個人ID情報、ID<sub>M</sub>…装置ID情報、Au1, Au2…認証装置の署名情報、Z…受注者の個人キー情報、Inf1…認証要求、Inf4…認証応答

301…トランザクション認証システム、311…発注者端末装置、315…受注者端末装置、340, 341…ネットワーク銀行、350, 351…認証装置、361, 371, 381, 391…受信部、362, 372, 382, 392…送信部、363, 373, 383, 393…暗号化部、364, 374, 384, 394…復号部、365, 375, 385, 395…記憶部、366, 376, 386, 396…制御部、367, 377…署名検証部、387, 397…署名作成部、388, 398…課金処理部

a1…発注情報、k1…発注者31の個人キー情報k1、ID1…発注者31の個人ID情報、b1…受注者を特定する情報、Au-B…認証装置51の署名情報、Au-A1, Au-A2…認証装置50の署名情報、Z…受注者の個人キー情報

401…トランザクション認証システム、411…発注者端末装置、415…受注者端末装置、440…ネットワーク銀行、450…認証装置、461, 471, 481…受信部、462, 472, 482…送信部、463, 473, 483…暗号化部、464, 474, 484…復号部、465, 475, 485…記



憶部、466, 476, 486…制御部、467, 477…署名検証部、, 487…署名作成部、488…課金処理部、a1…発注情報、k1…発注者31の個人キー情報k1、ID1…発注者31の個人ID情報、ID<sub>N</sub>…ネットワークID、Au1, Au2…認証装置の署名情報、Z…受注者の個人キー情報、Inf1…認証要求、Inf4…認証応答

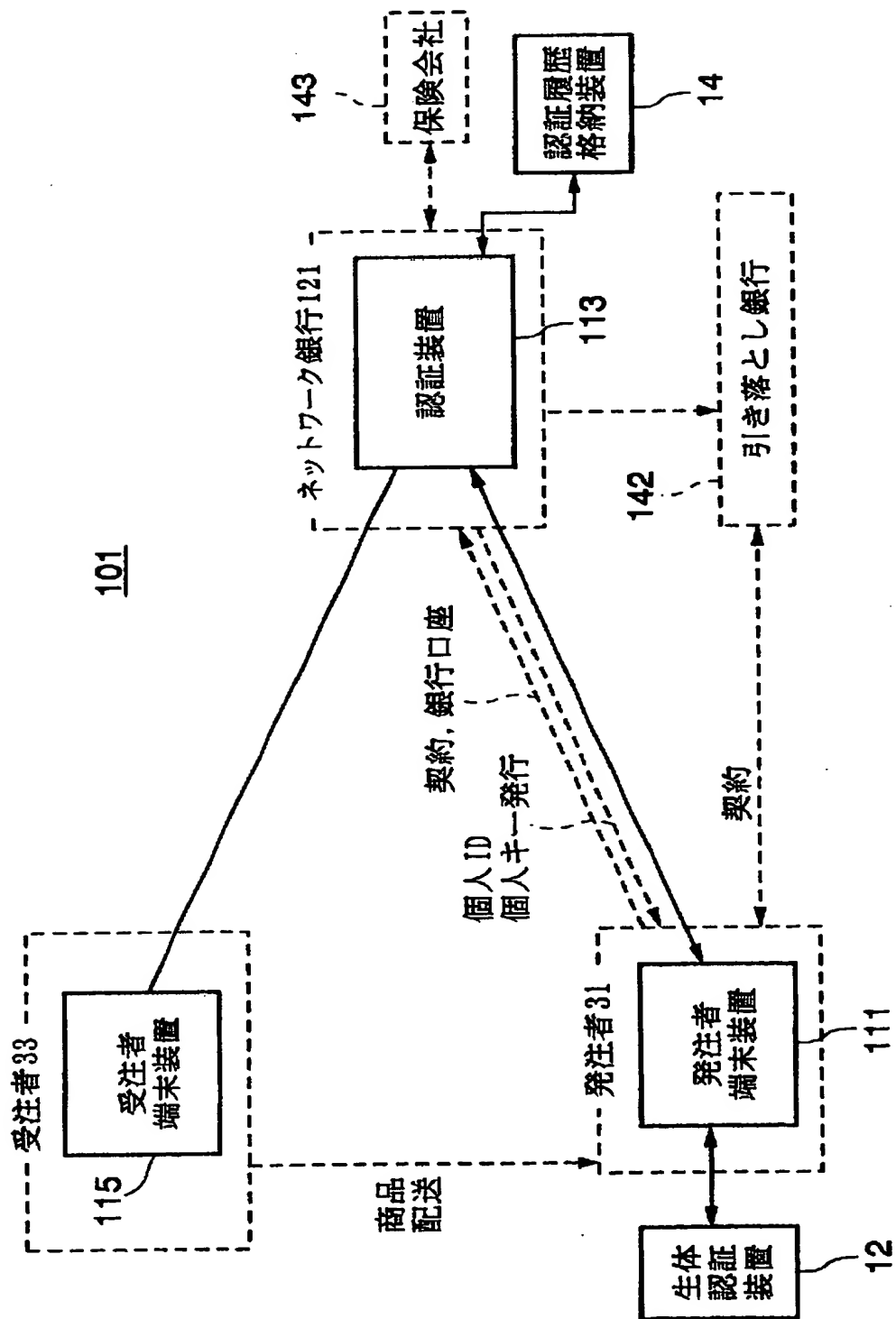
501…トランザクション認証システム、511…発注者端末装置、515…受注者端末装置、540…ネットワーク銀行、550…認証装置、561…外部ネットワークI/F、562…内部ネットワークI/F、571, 581…受信部、572, 582…送信部、563, 573, 583…暗号化部、564, 574, 584…復号部、565, 575, 585…記憶部、566, 576, 586…制御部、567, 577…署名検証部、, 587…署名作成部、588…課金処理部、a1…発注情報、k1…発注者31の個人キー情報k1、ID1…発注者31の個人ID情報、ID<sub>M1</sub>, ID<sub>M2</sub>, ID<sub>M3</sub>, ID<sub>M4</sub>, ID<sub>M56</sub>…装置ID情報、Au1, Au2…認証装置の署名情報、Z…受注者の個人キー情報、Inf1…認証要求、Inf4…認証応答

601…情報記録装置、610…読み出し回路、611…暗号化回路、612…情報分割回路、613, 614…書き込み回路、615, 616, 617…記録媒体、620, 621…読み出し回路、622…情報合成回路、623…復号回路、624…書き込み回路、631…情報復元装置、641…情報記録装置、650…読み出し回路、651…情報分割回路、652, 653…暗号化回路、654, 655…書き込み回路、661…情報復号装置、670, 671…読み出し回路、672, 673…復号回路、674…情報合成回路、675…書き込み回路

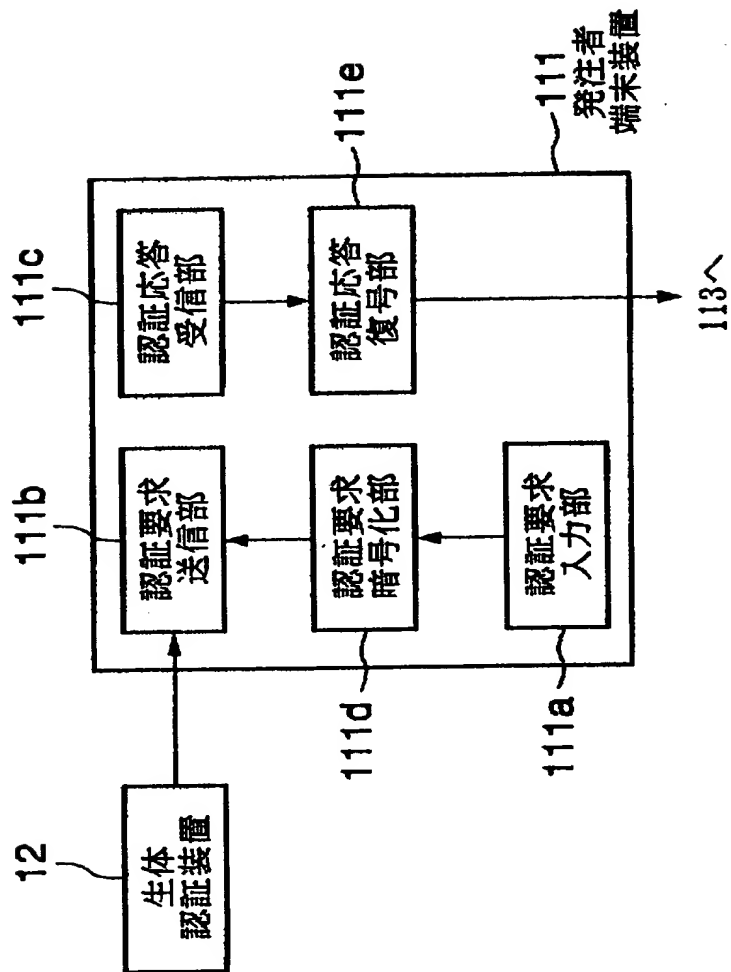
【書類名】

図面

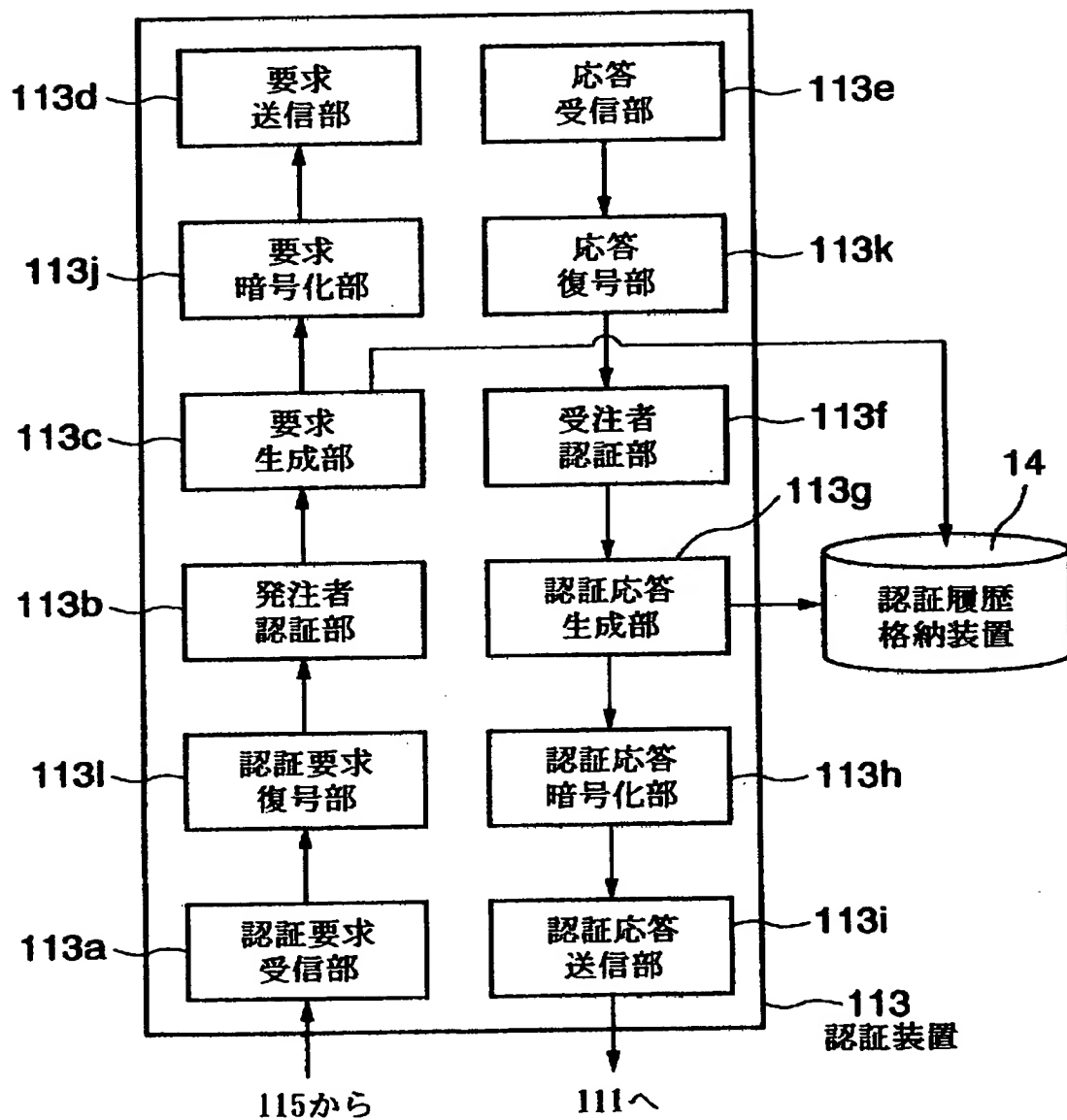
【図 1】



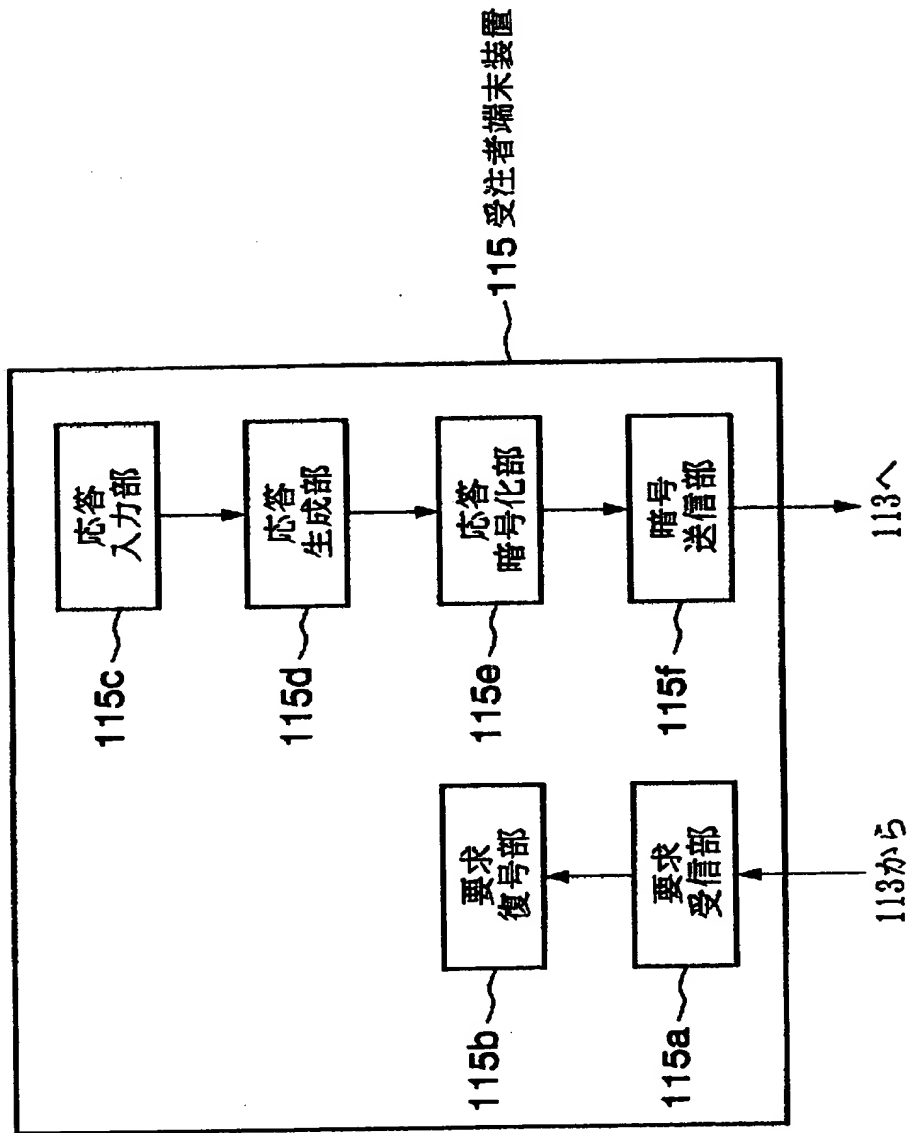
【図2】



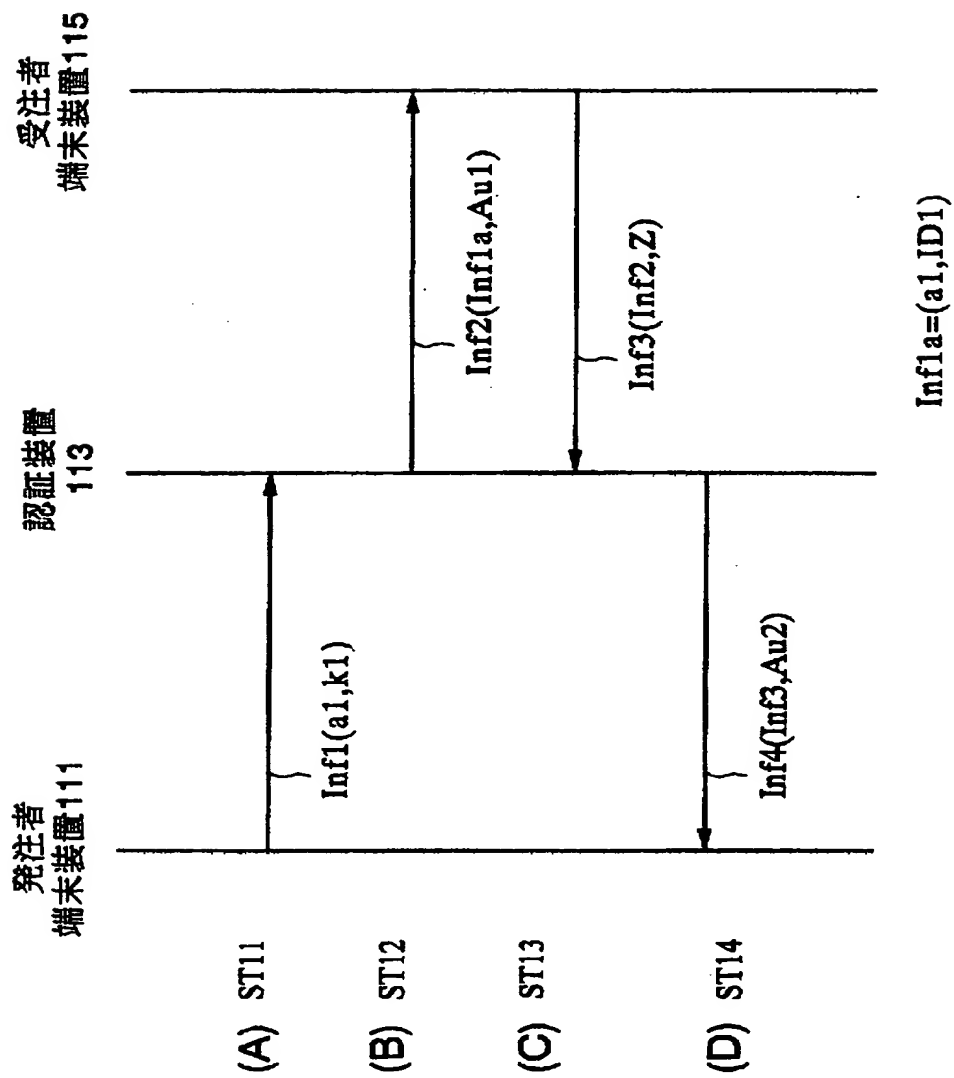
【図3】



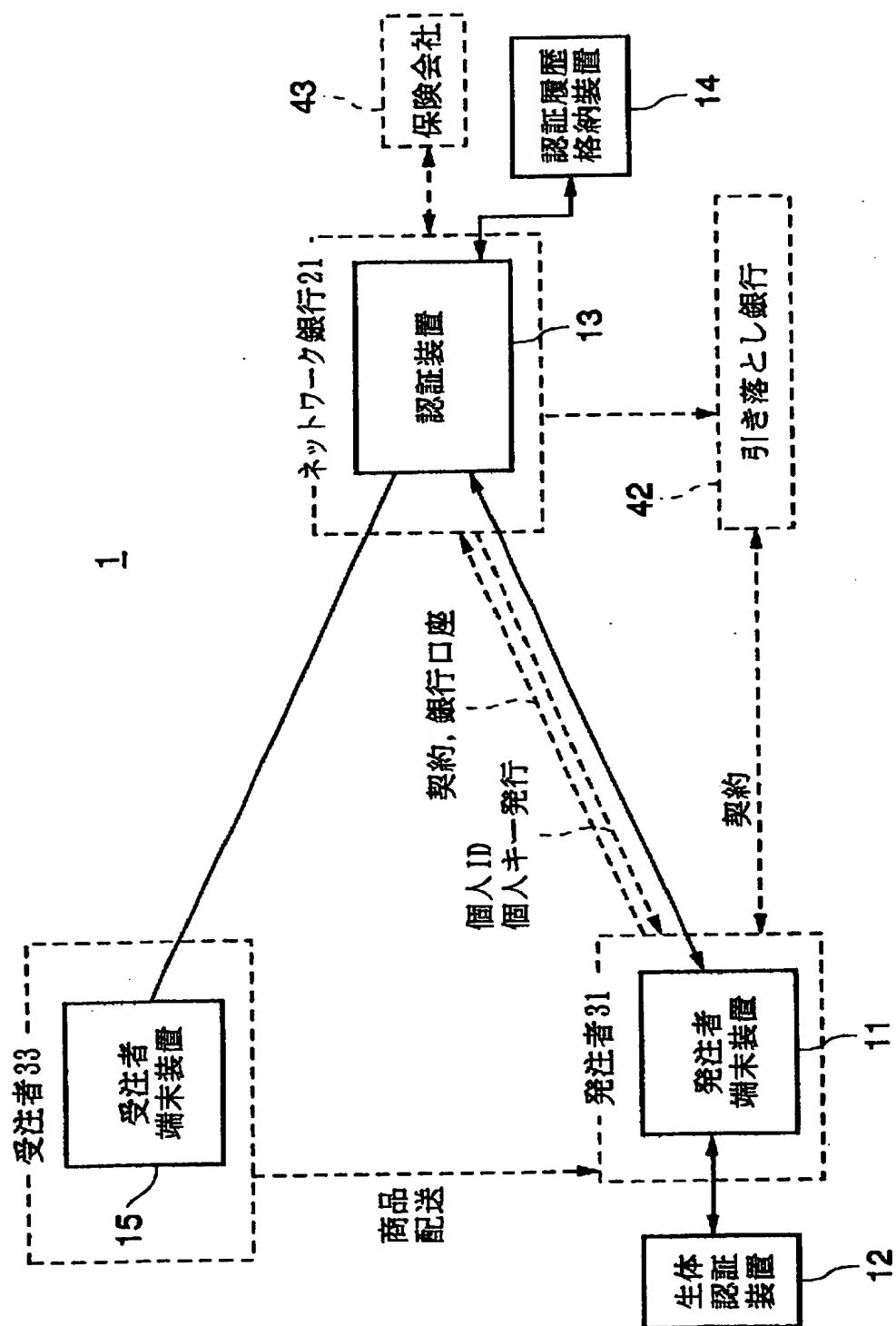
【図 4】



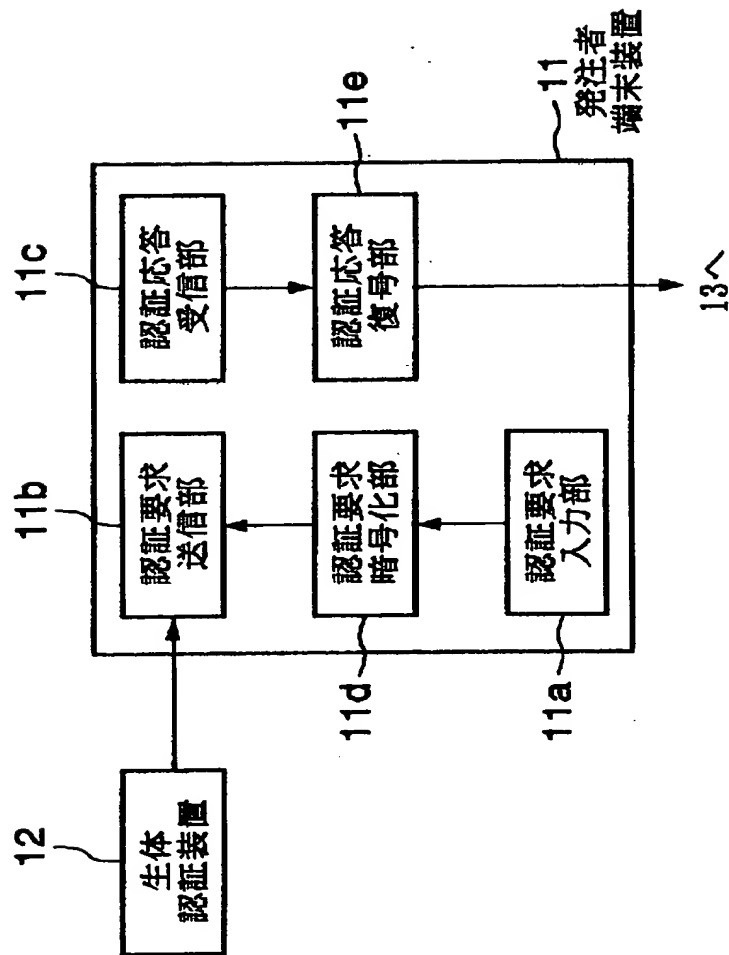
【図 5】



【図 6】

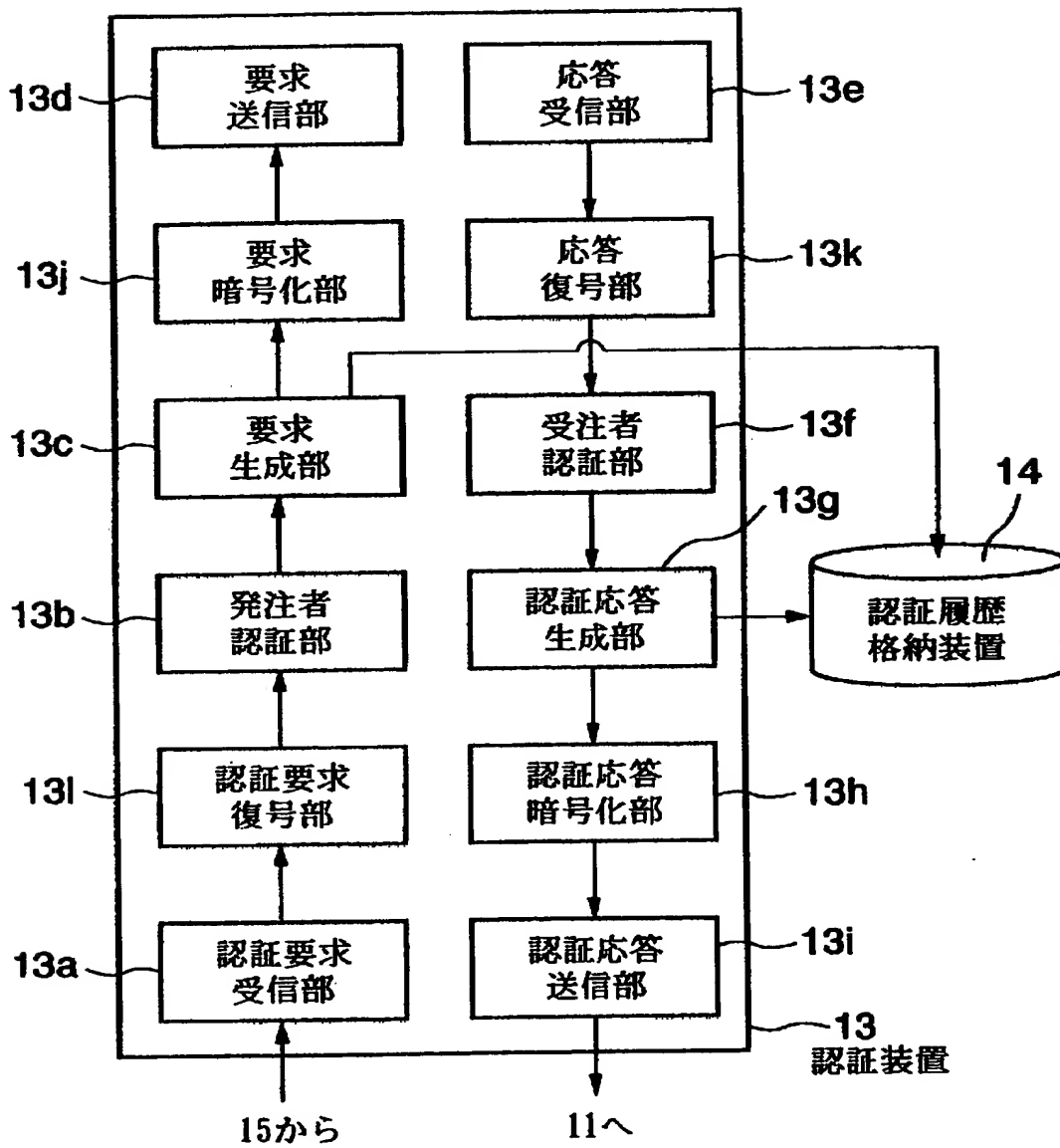


【図7】

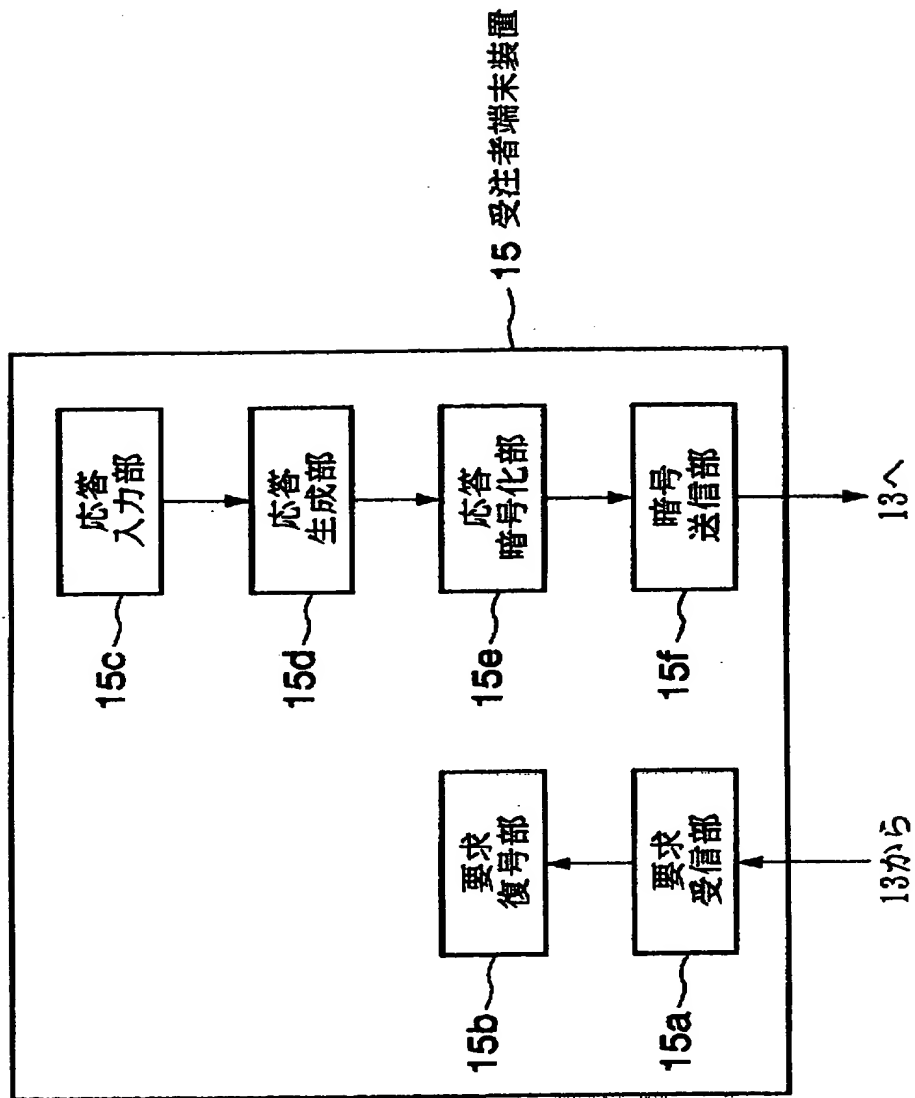




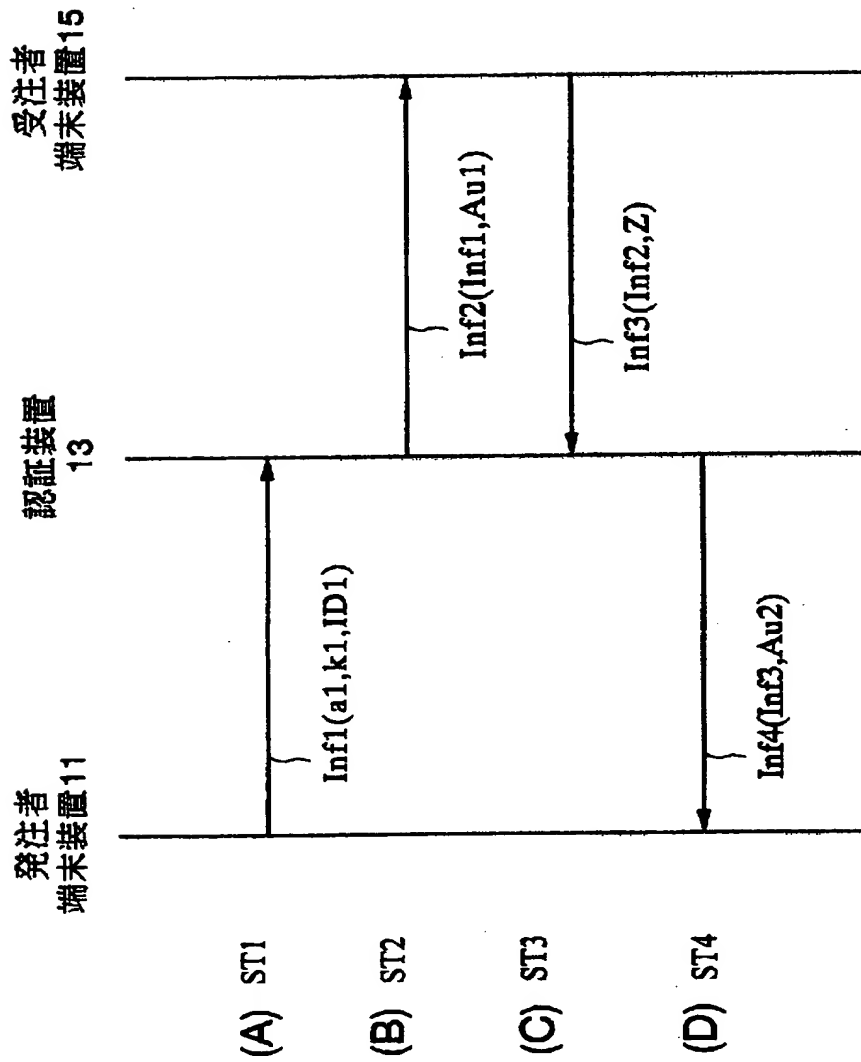
【図 8】



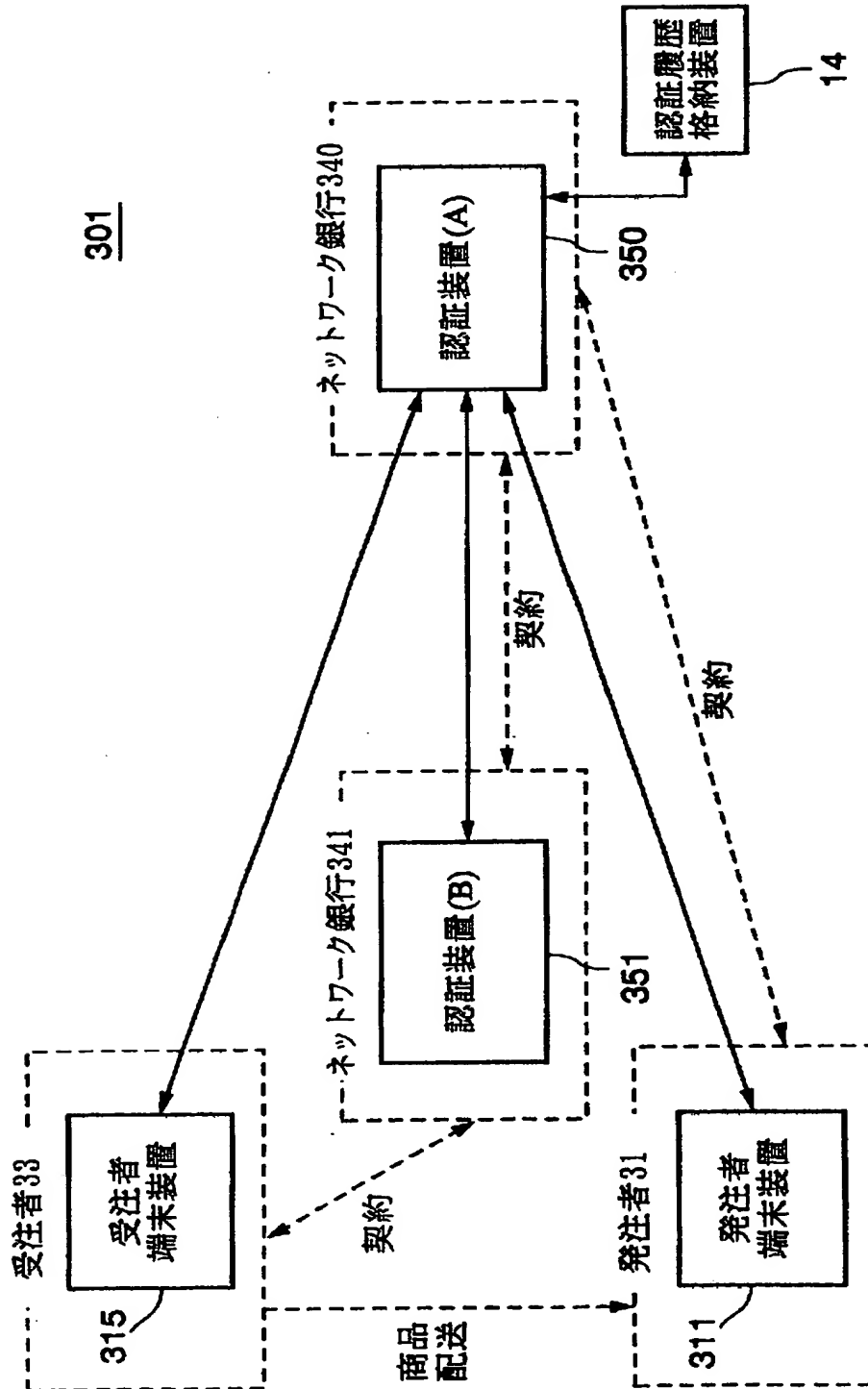
【図9】



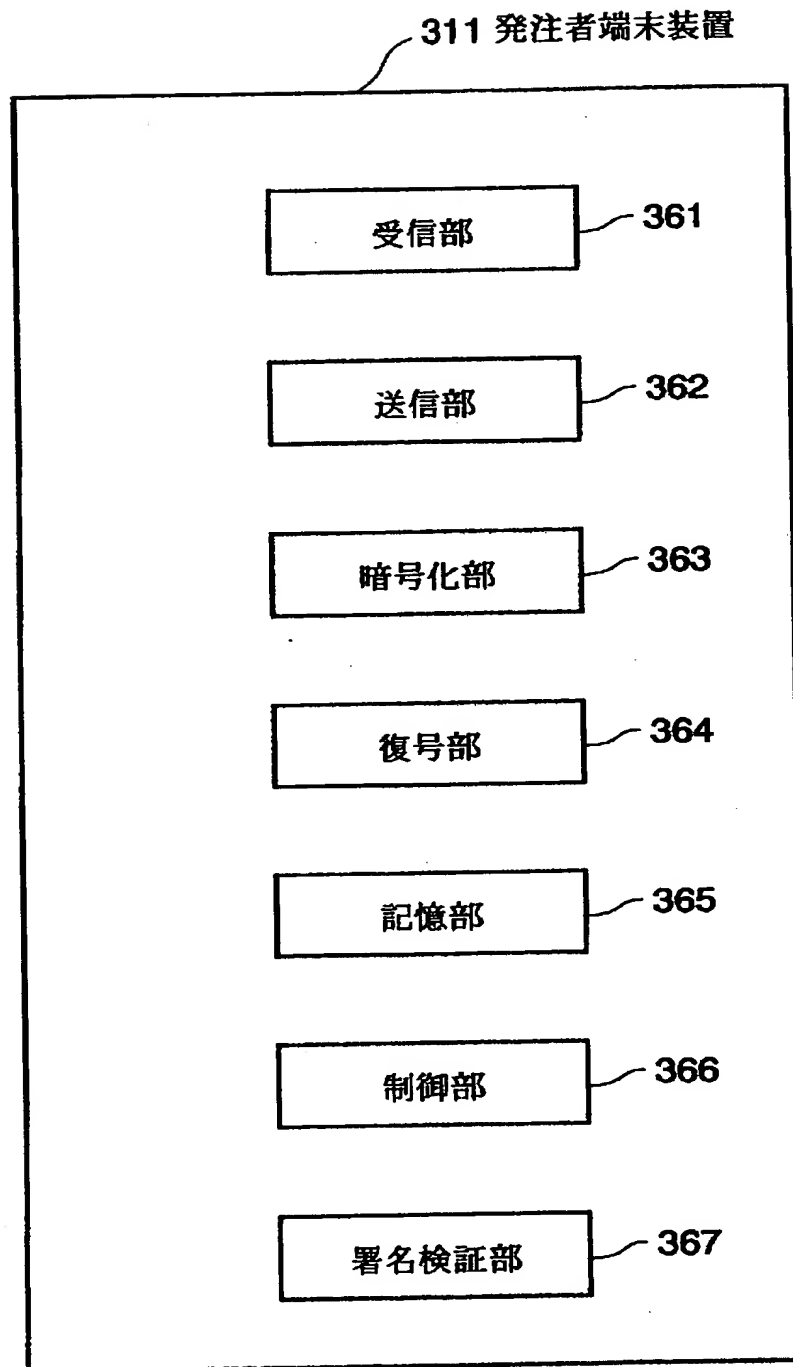
【図 1 0】



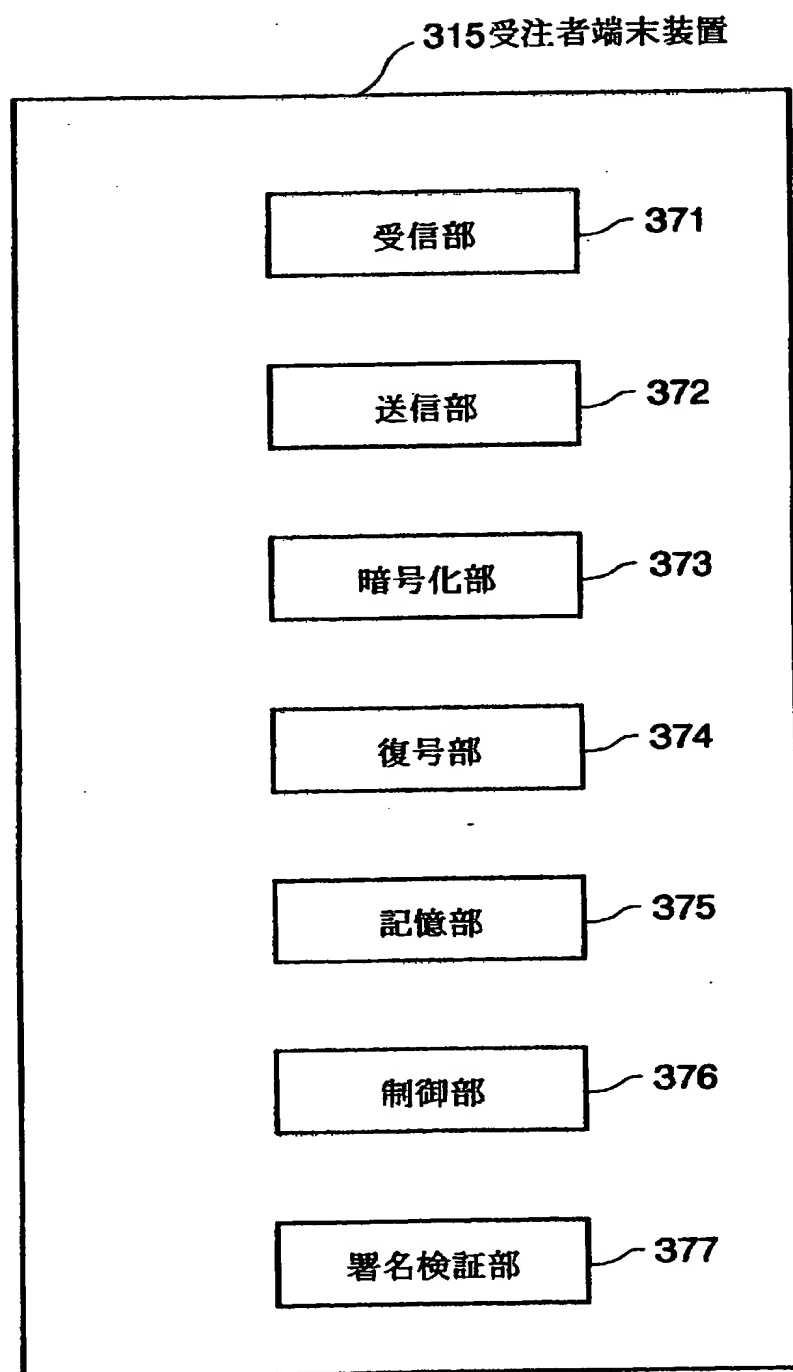
【図 1 1】



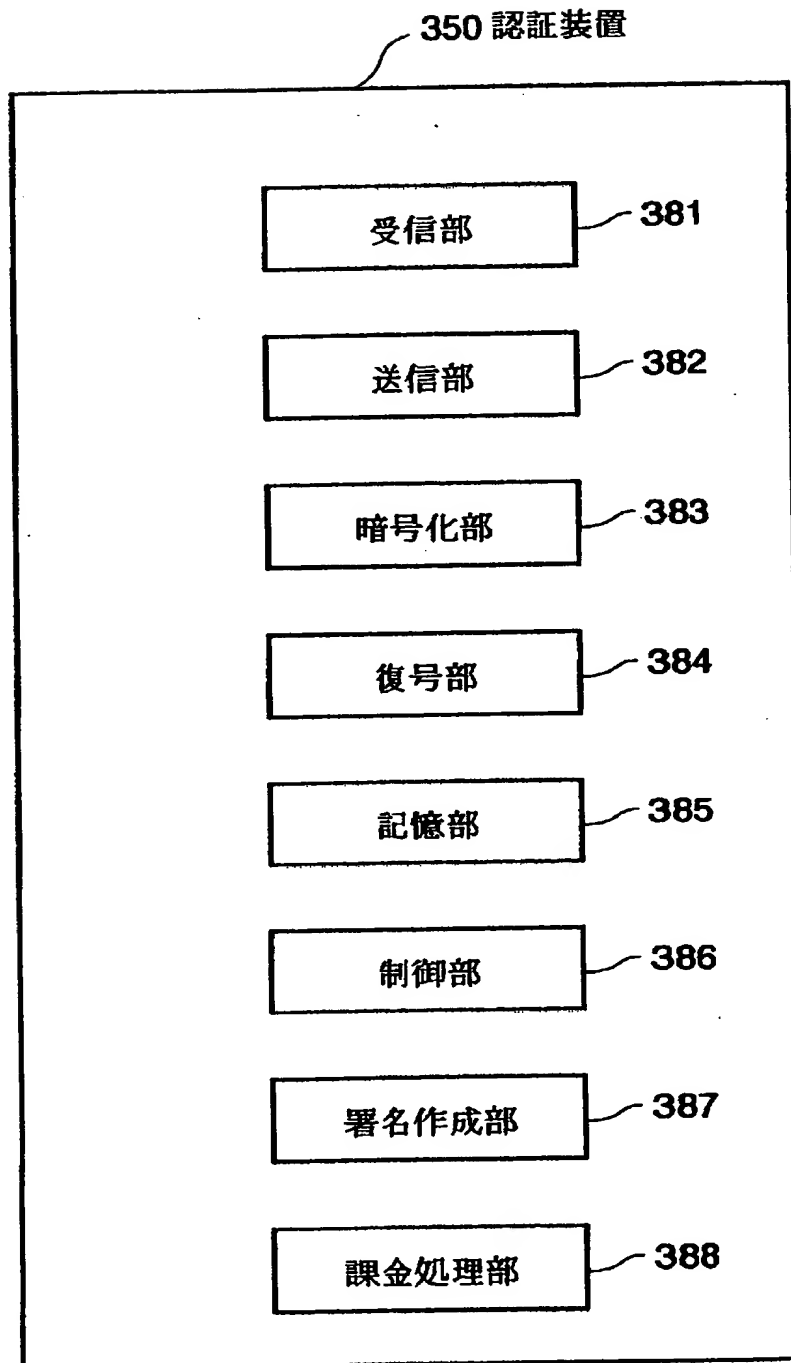
【図 12】



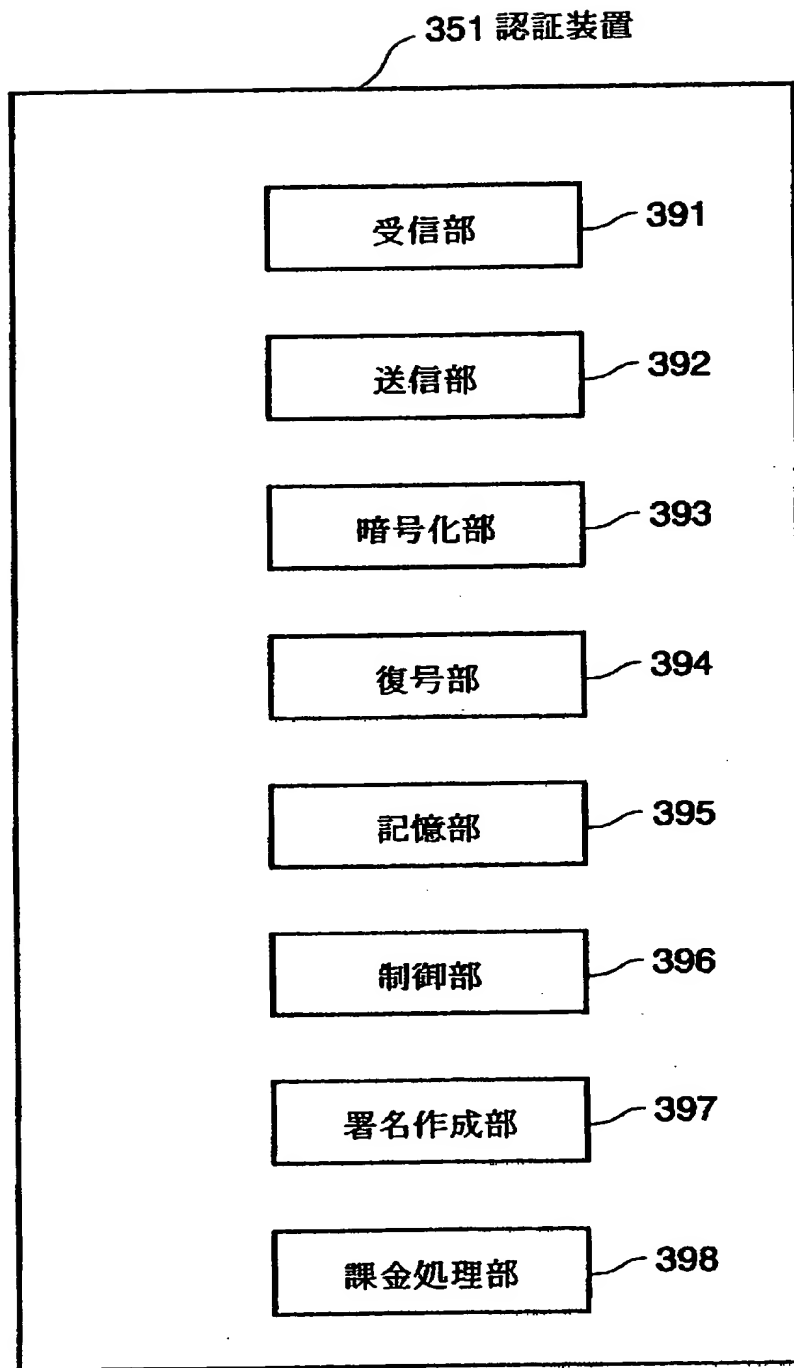
【図13】



【図 14】

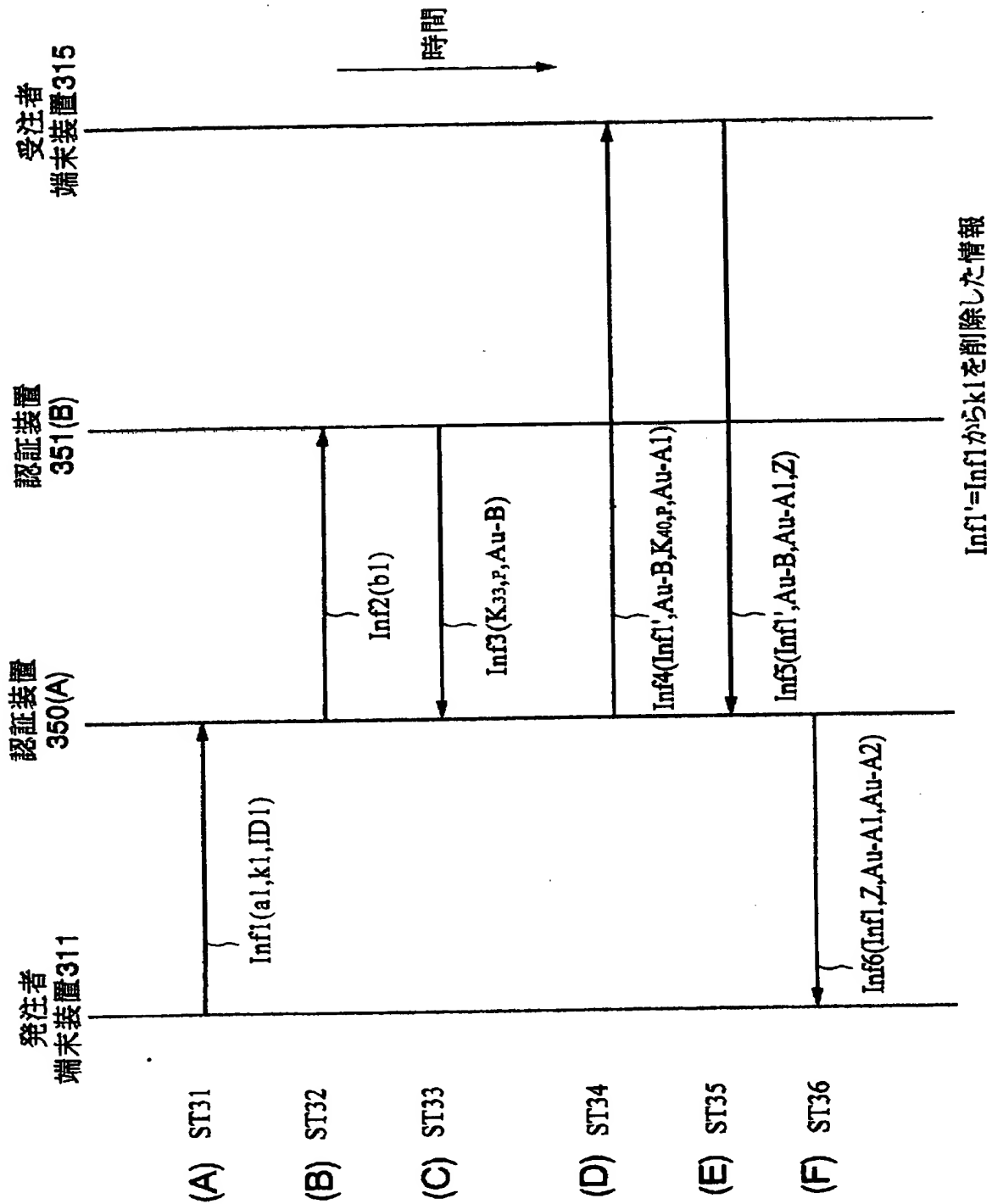


【図 15】

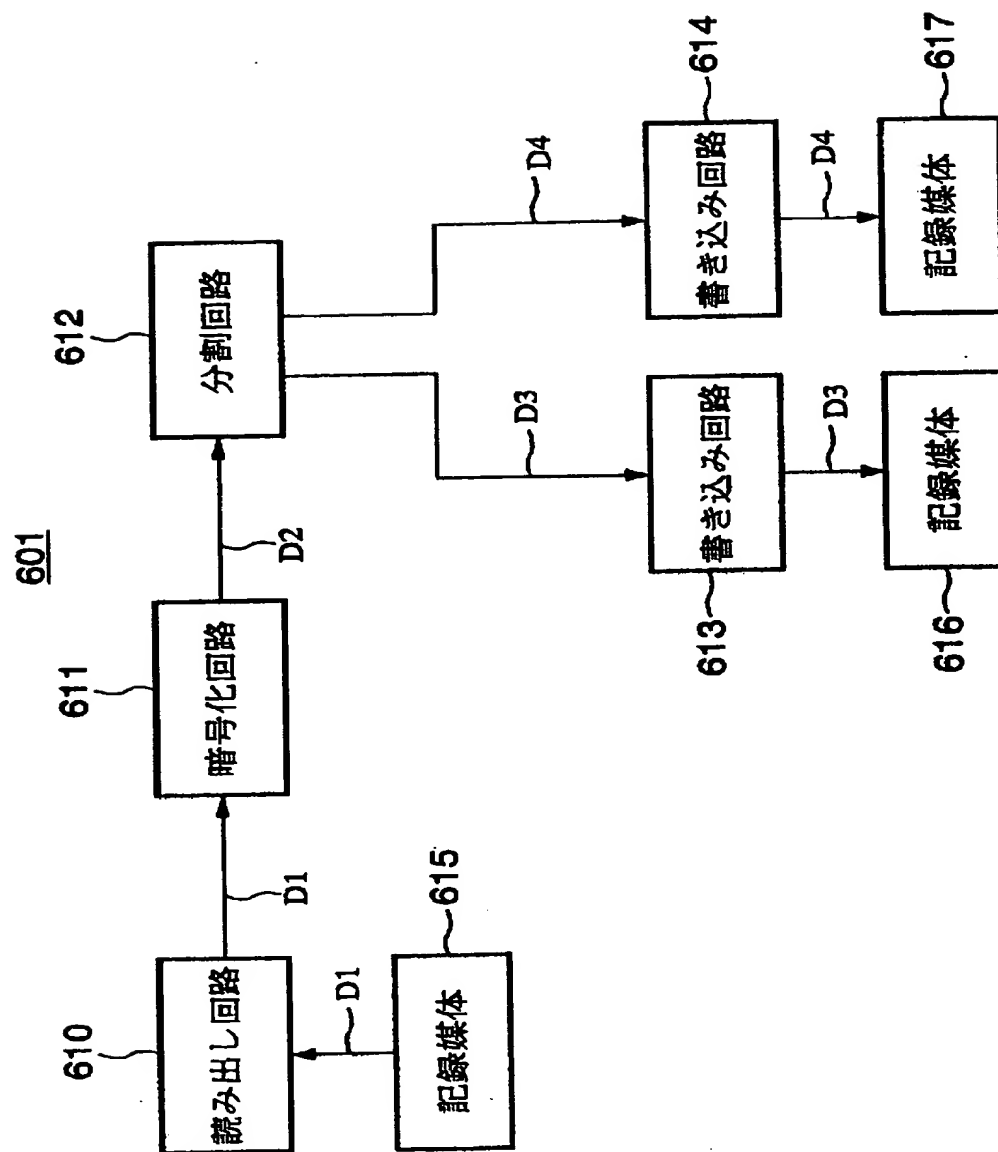




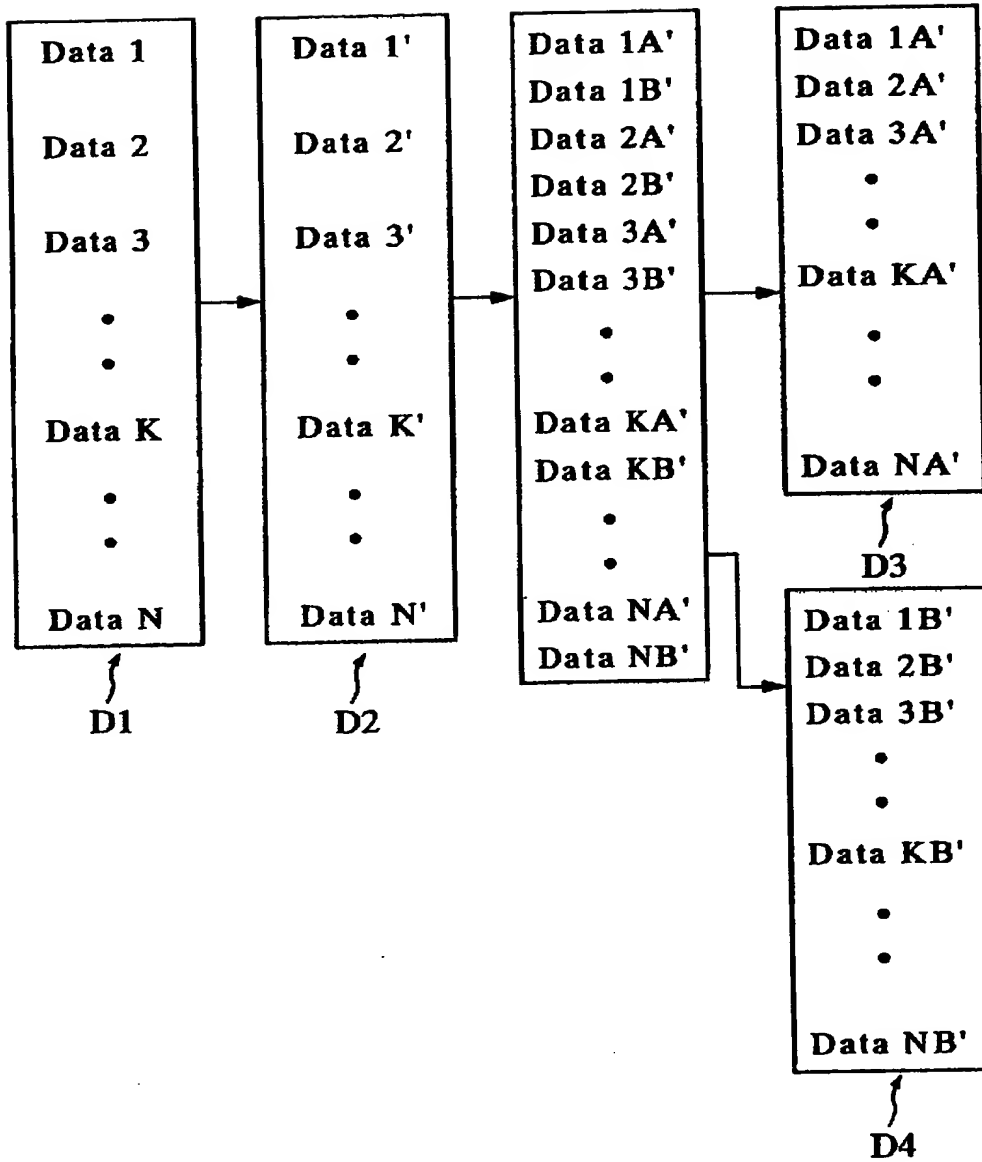
【図 16】



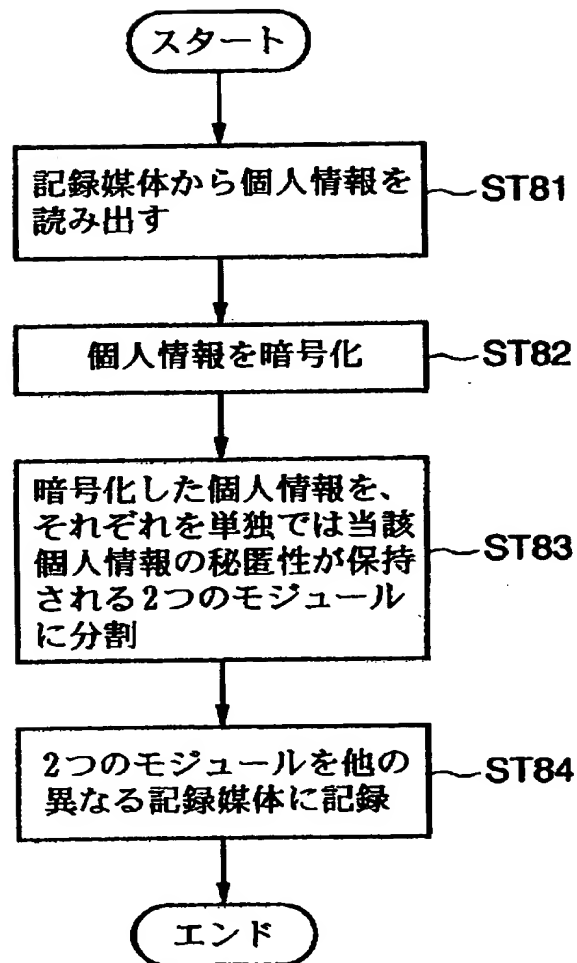
【図 17】



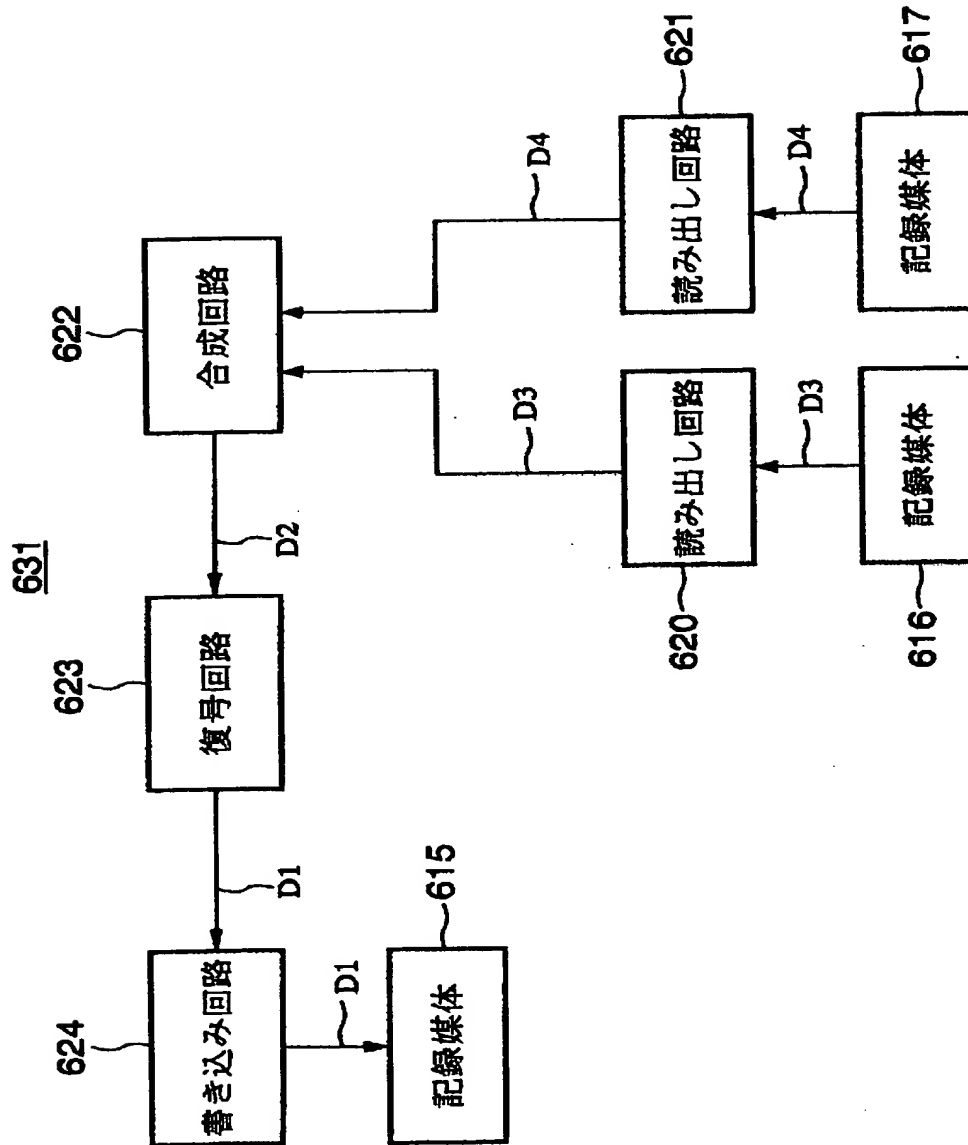
【図18】



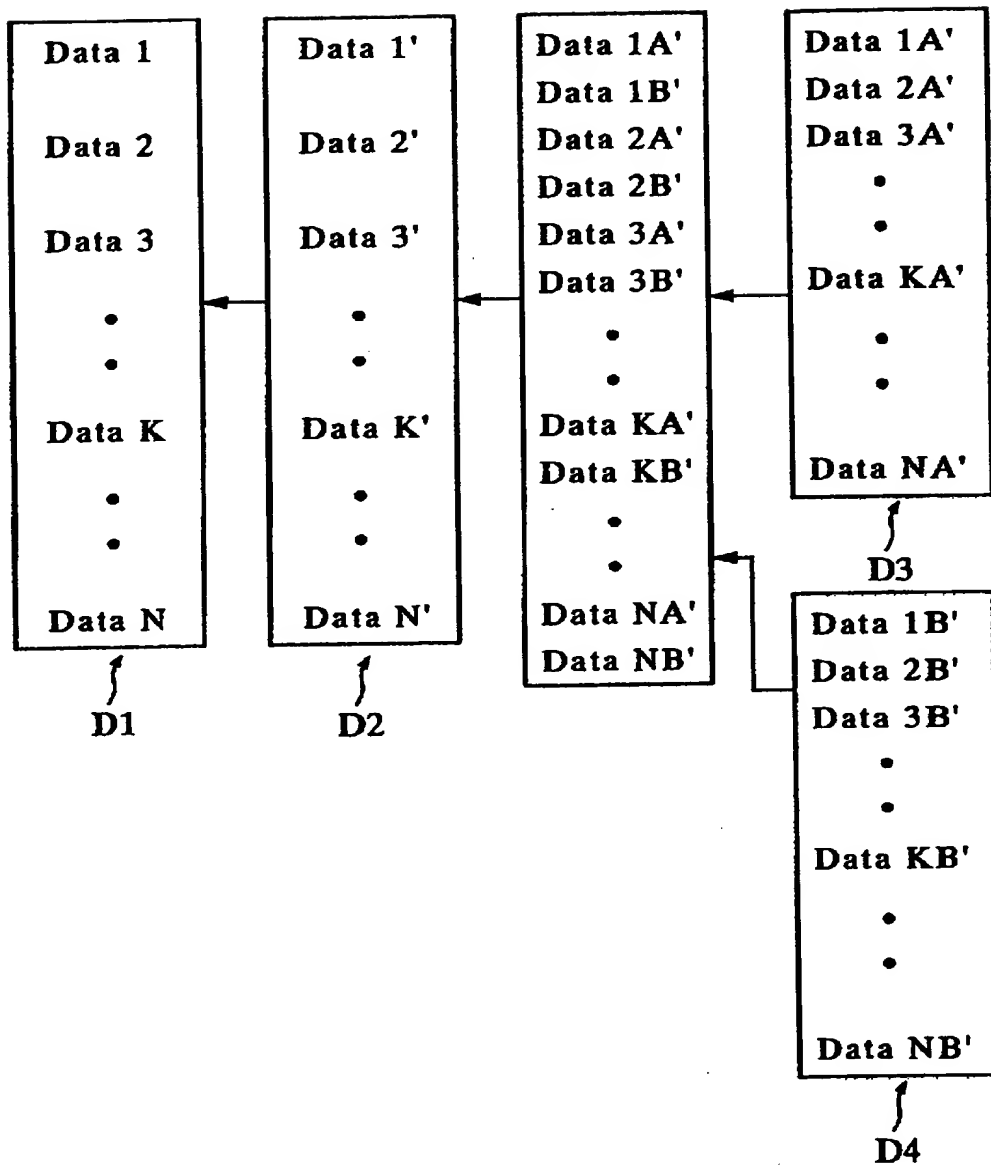
【図19】



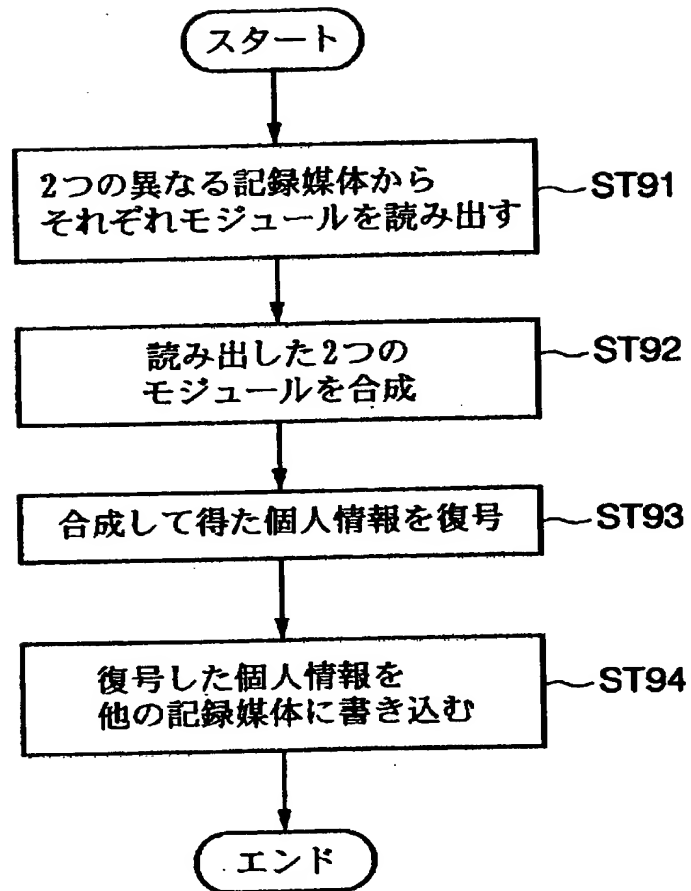
【図 20】



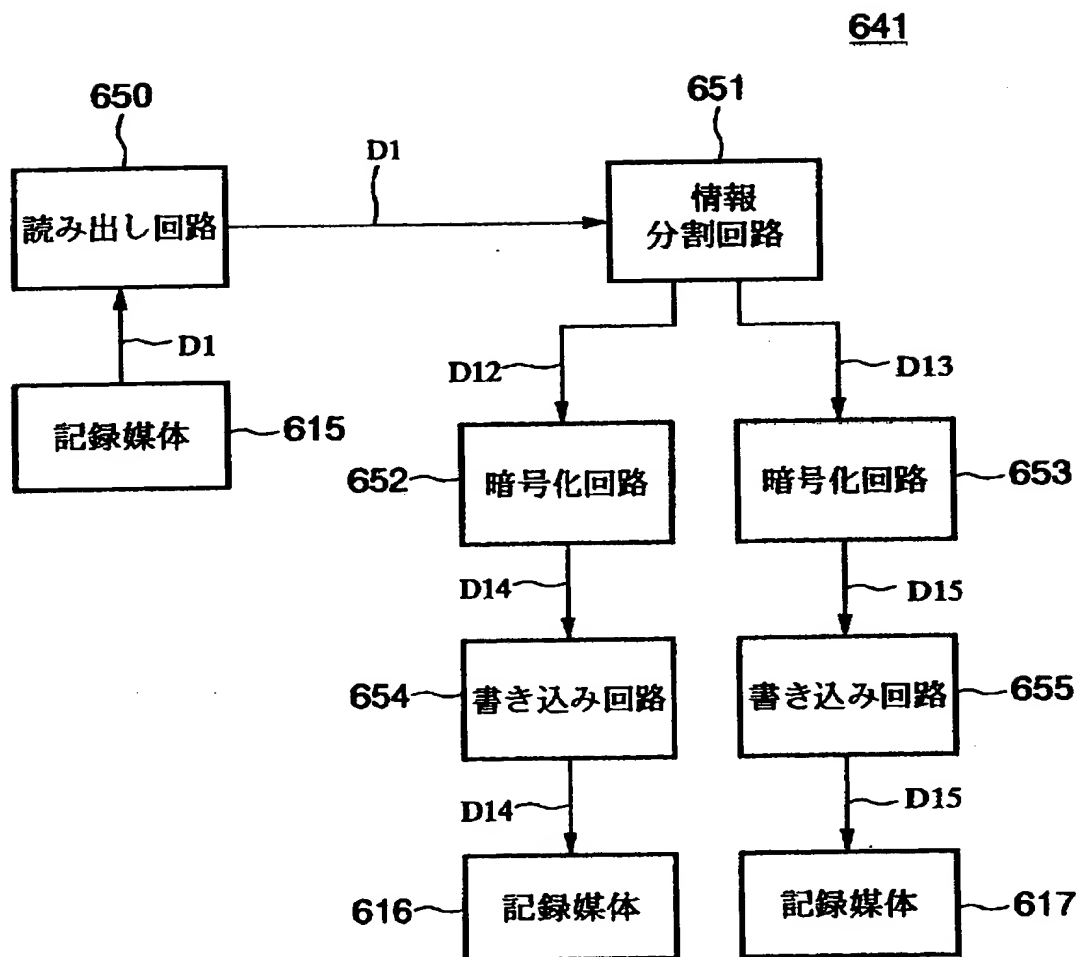
【図 21】



【図 22】

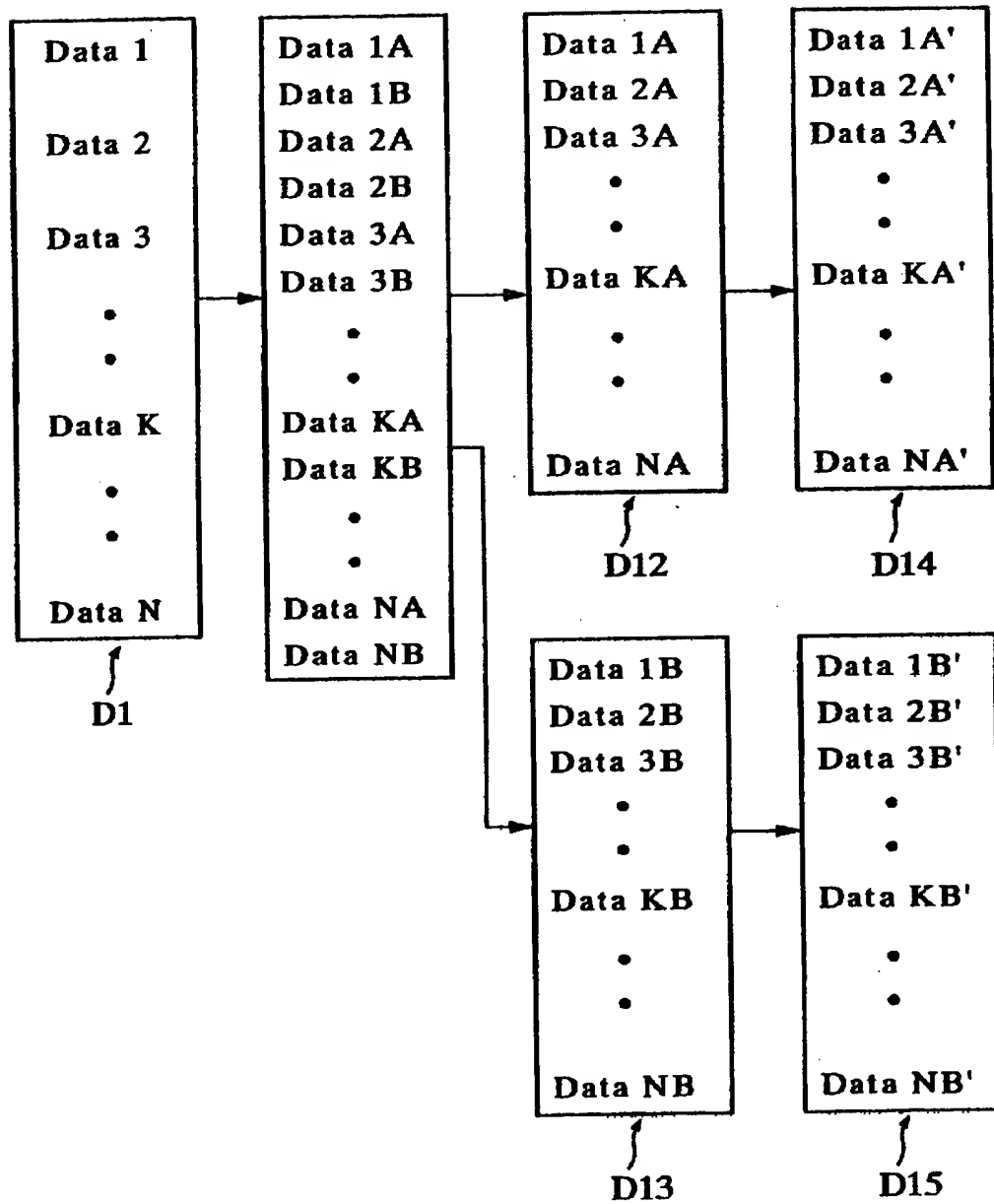


【図 23】

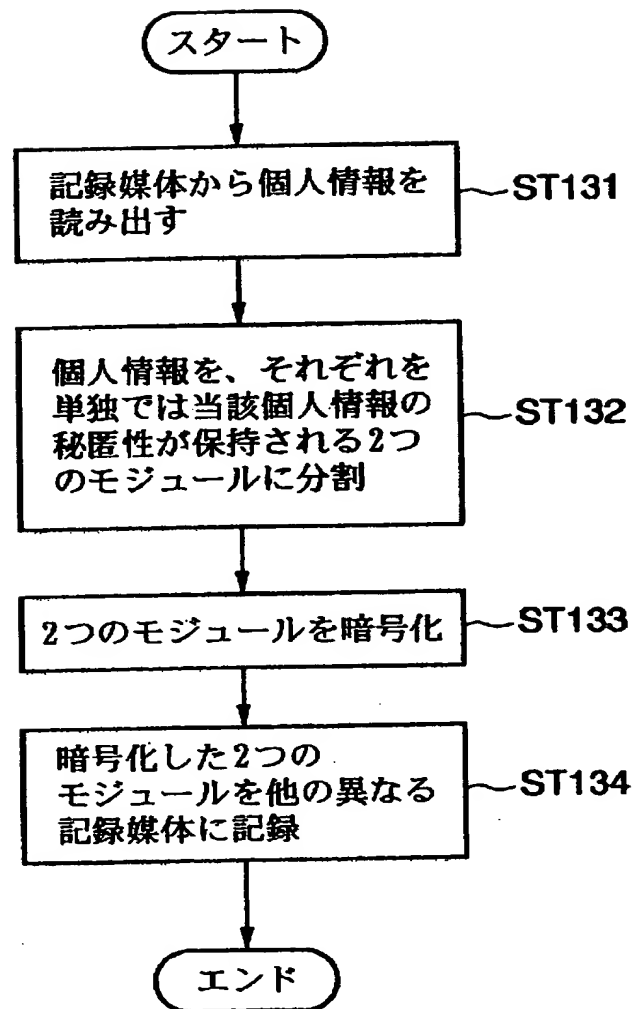




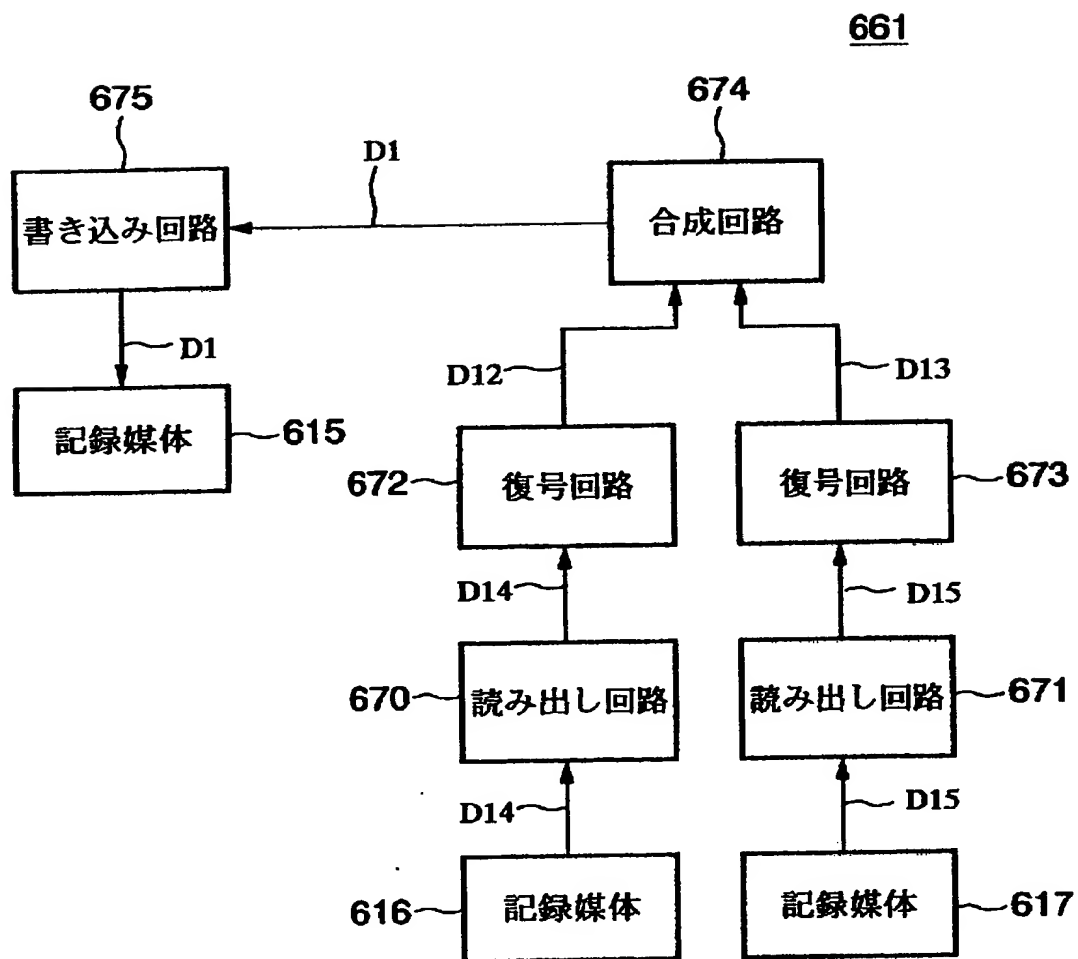
【図 24】



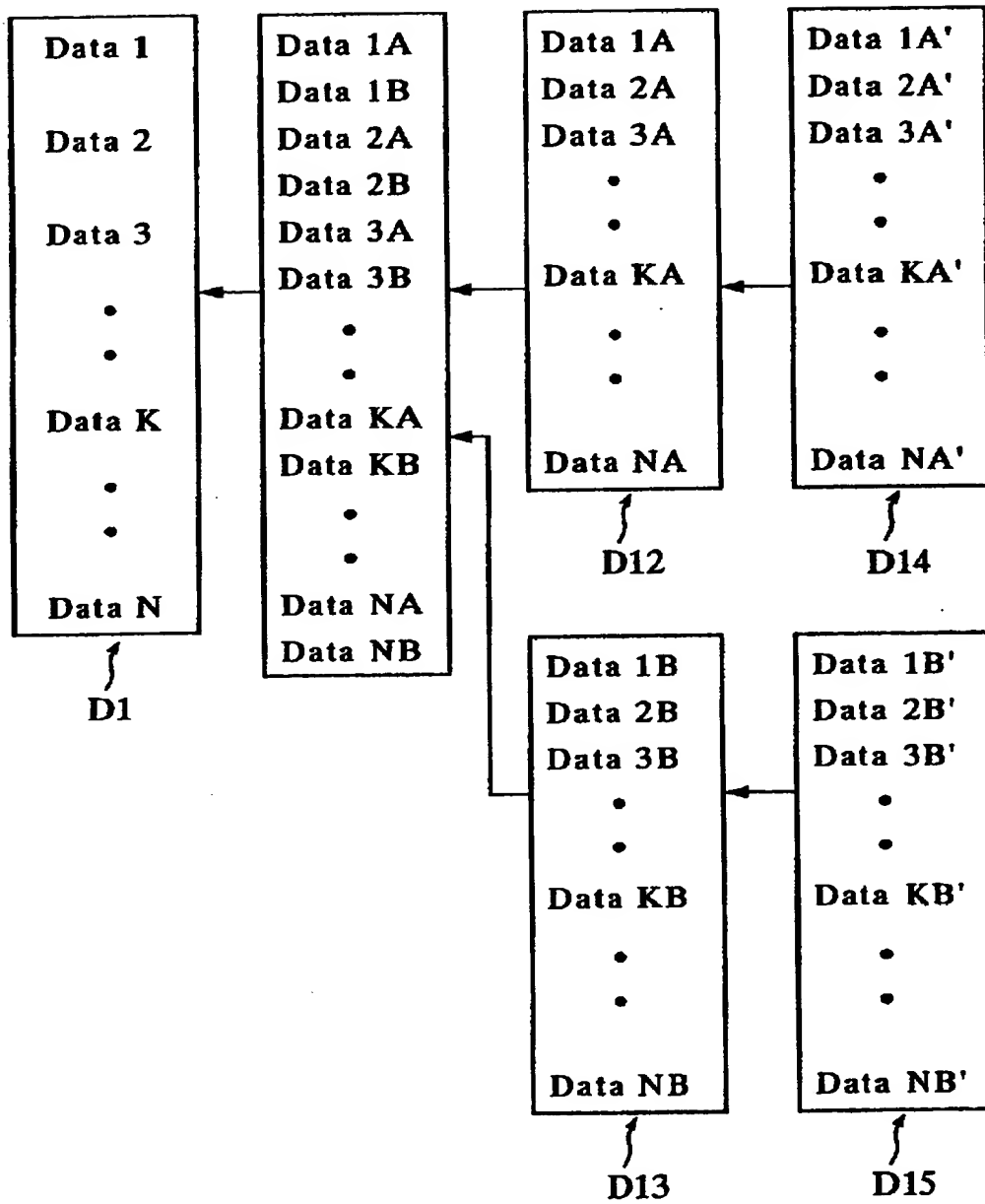
【図25】



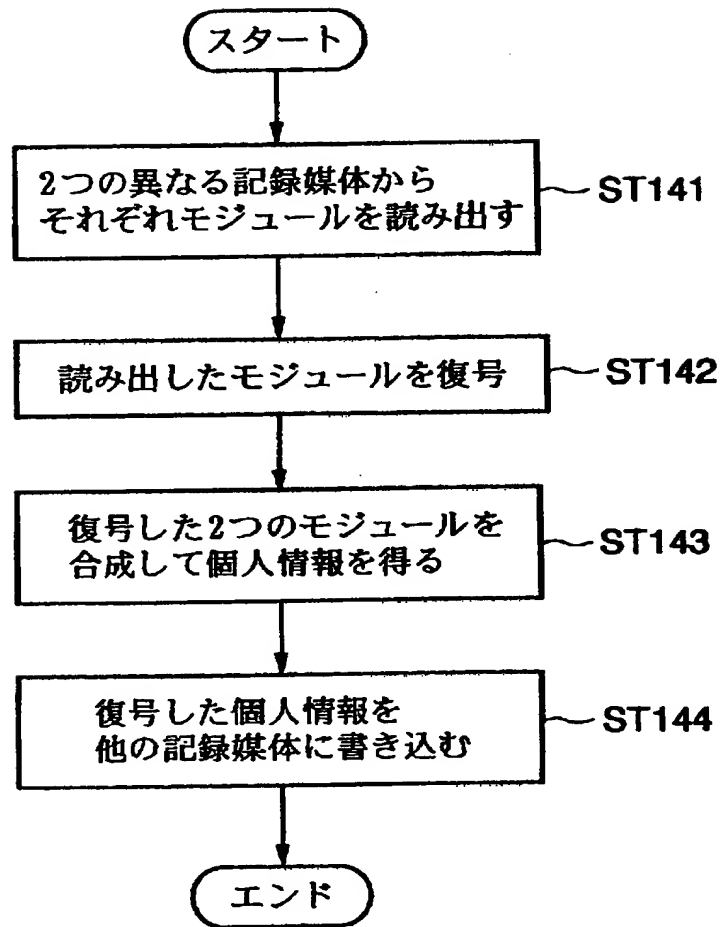
【図 26】



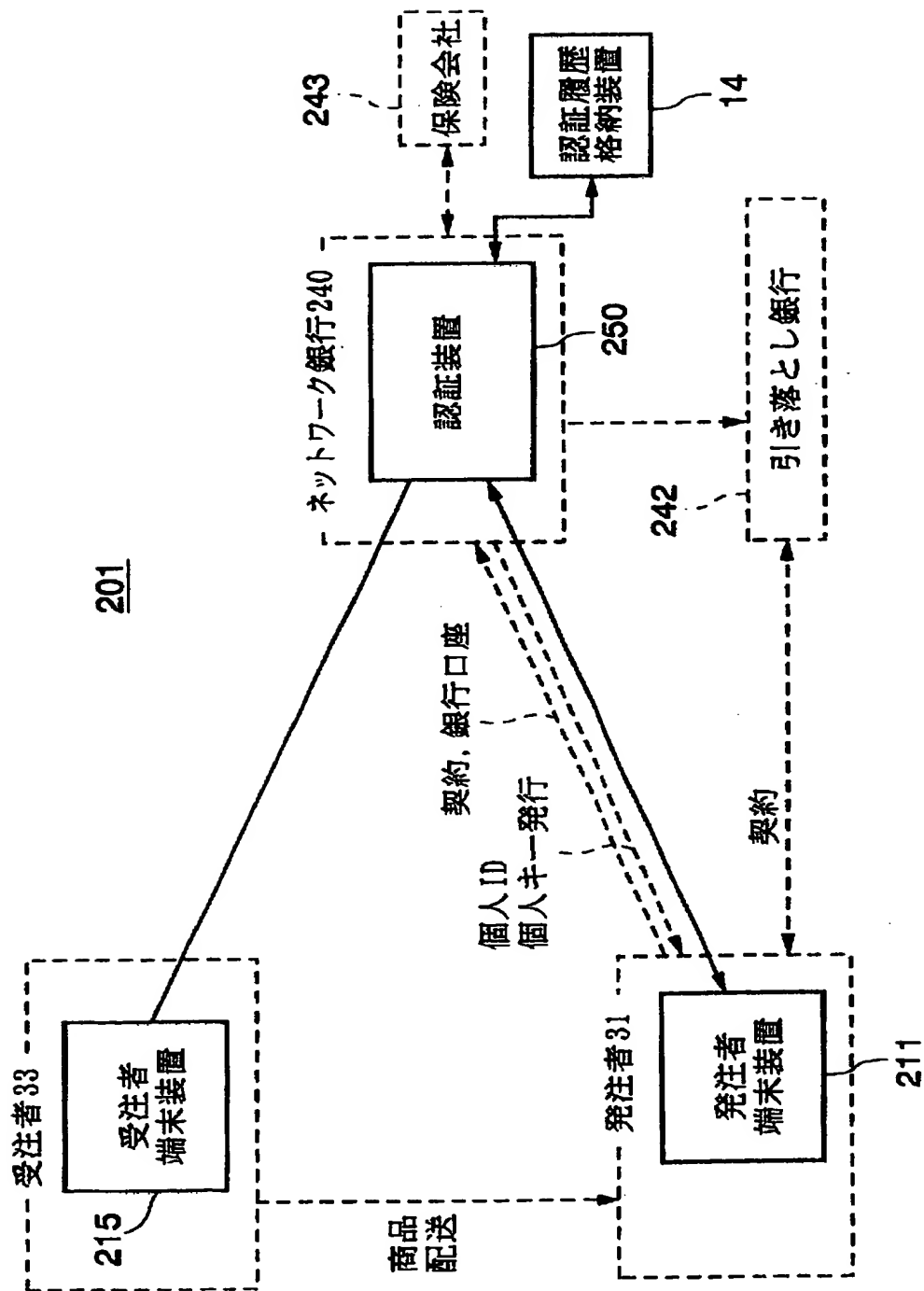
【図27】



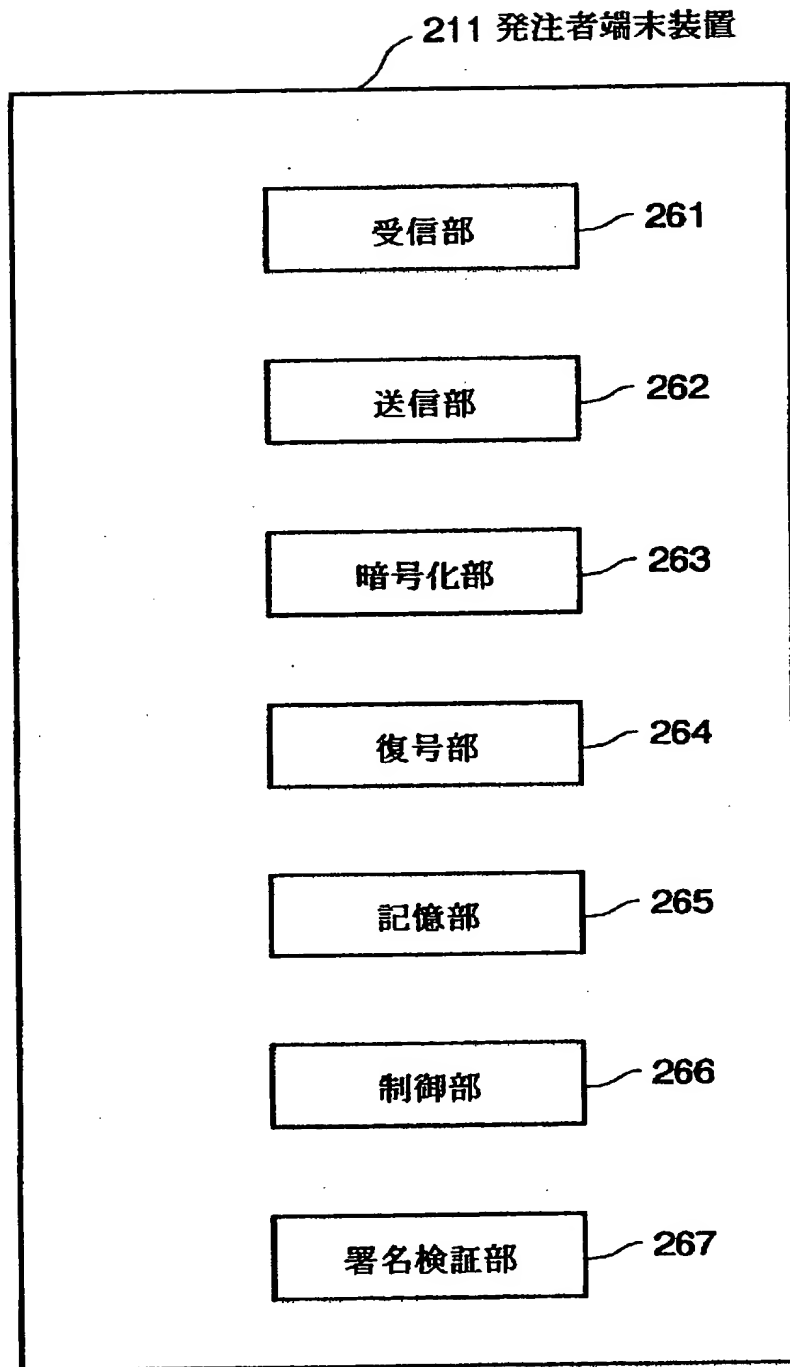
【図 28】



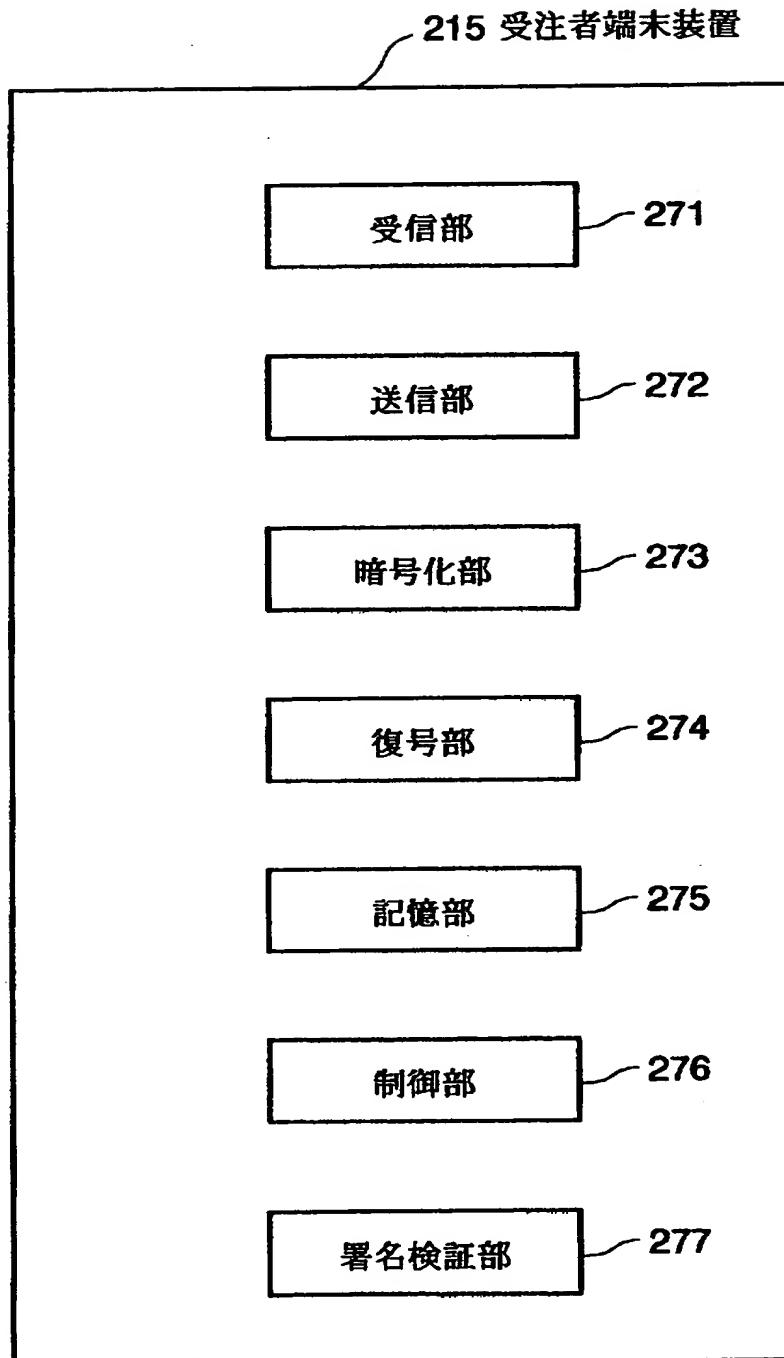
【図 29】



【図 30】

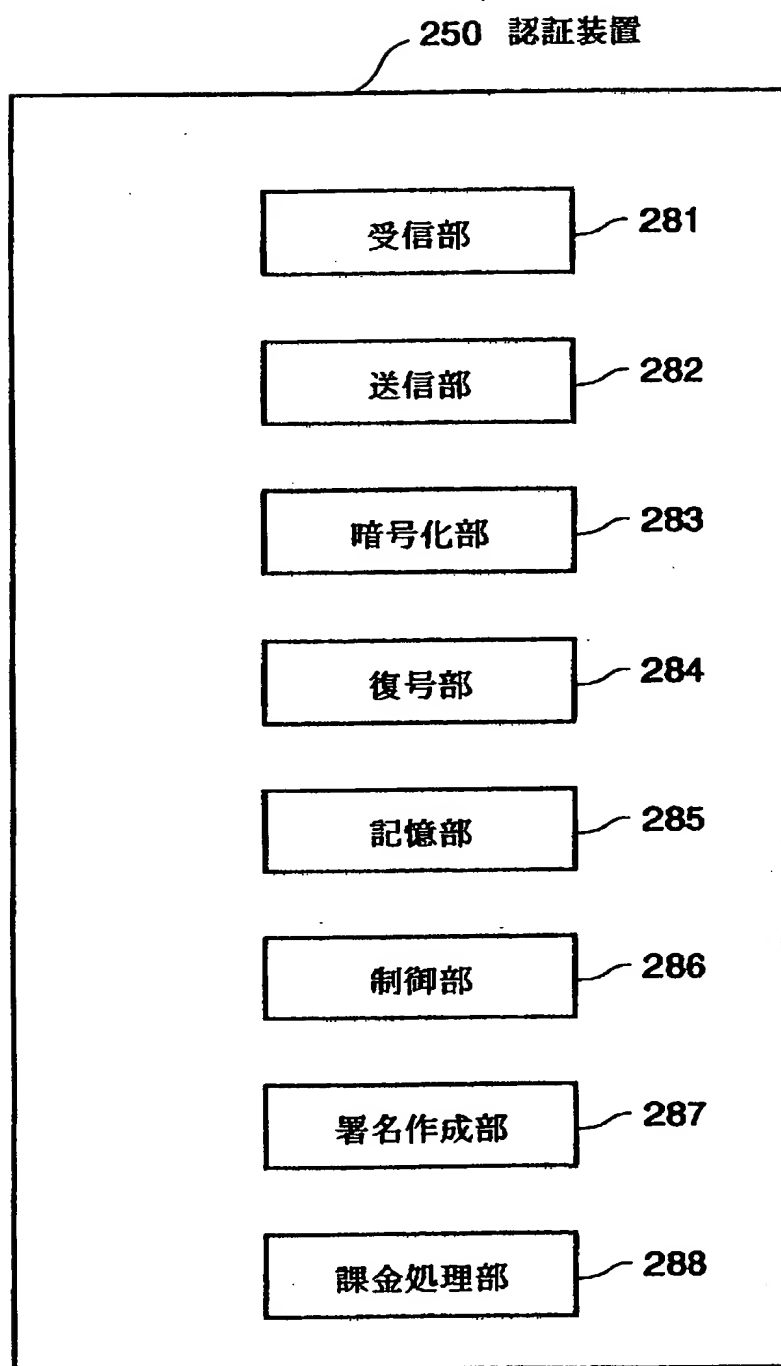


【図 31】

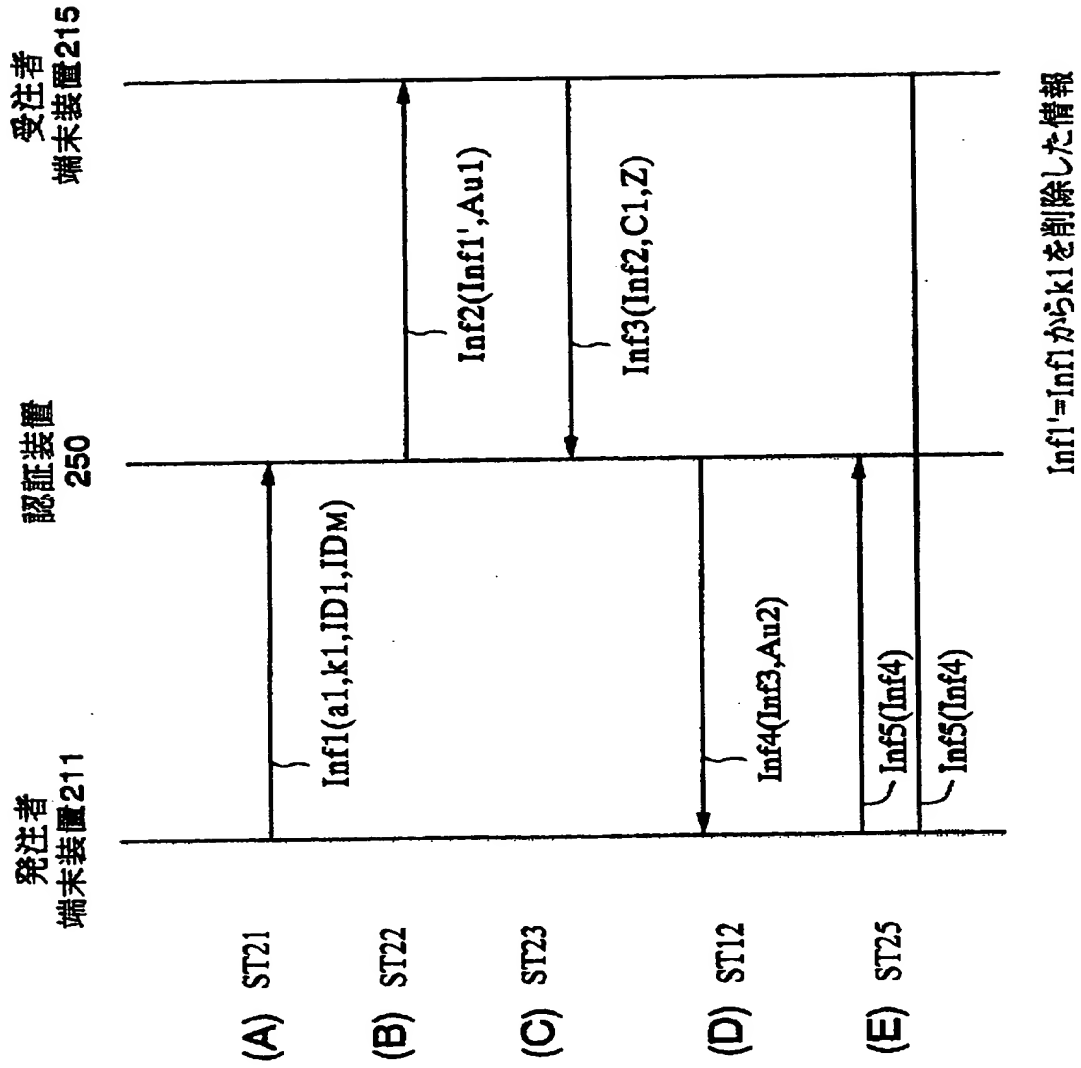




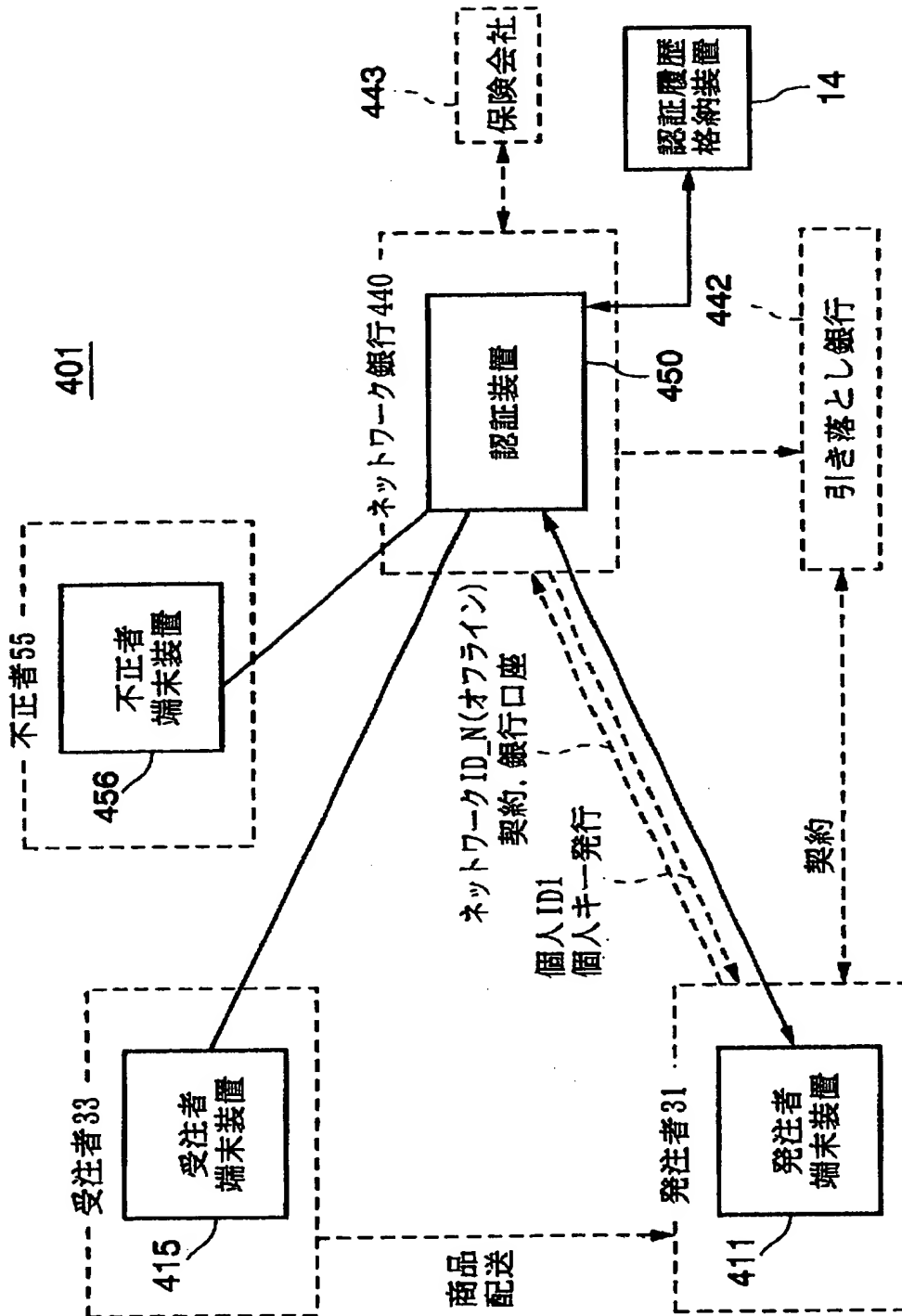
【図 32】



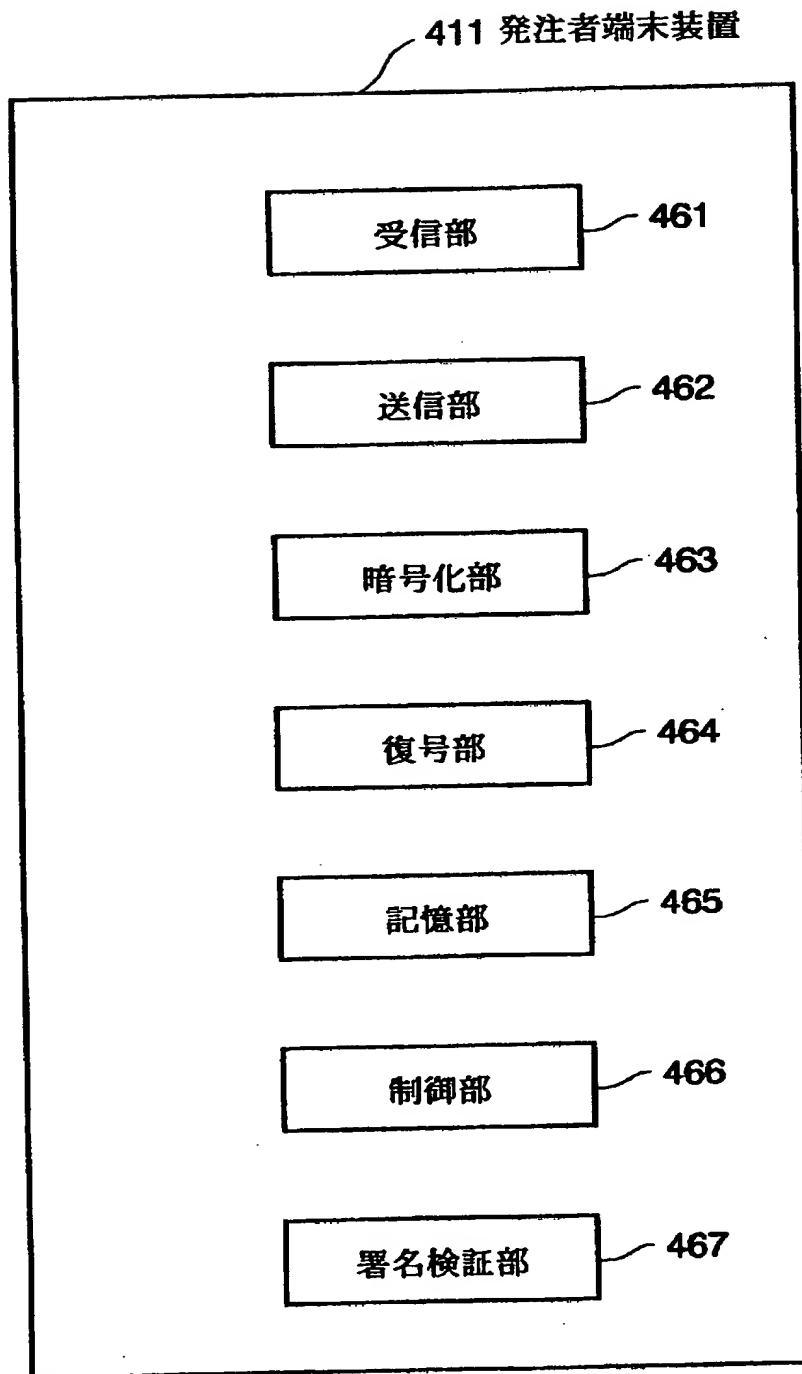
【図 3 3】



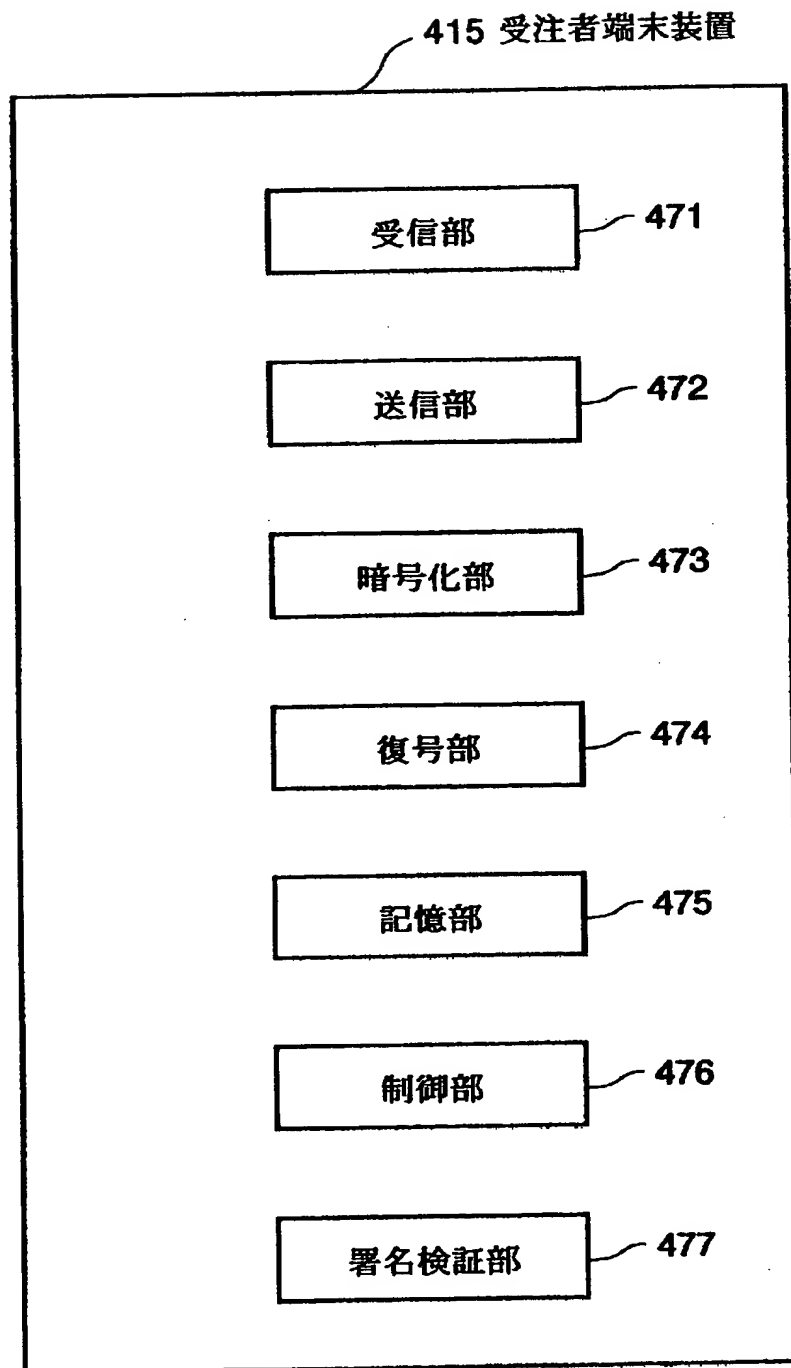
【図 3 4】



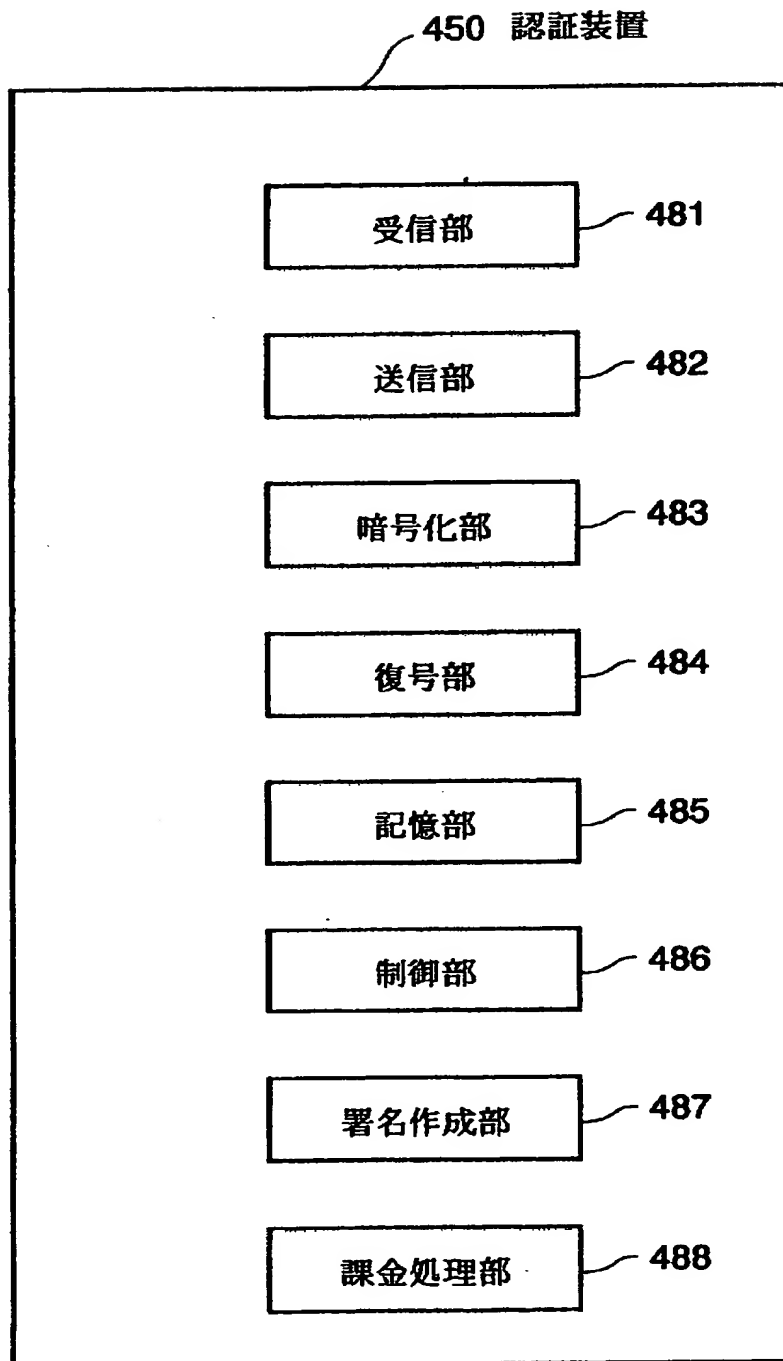
【図 3 5】



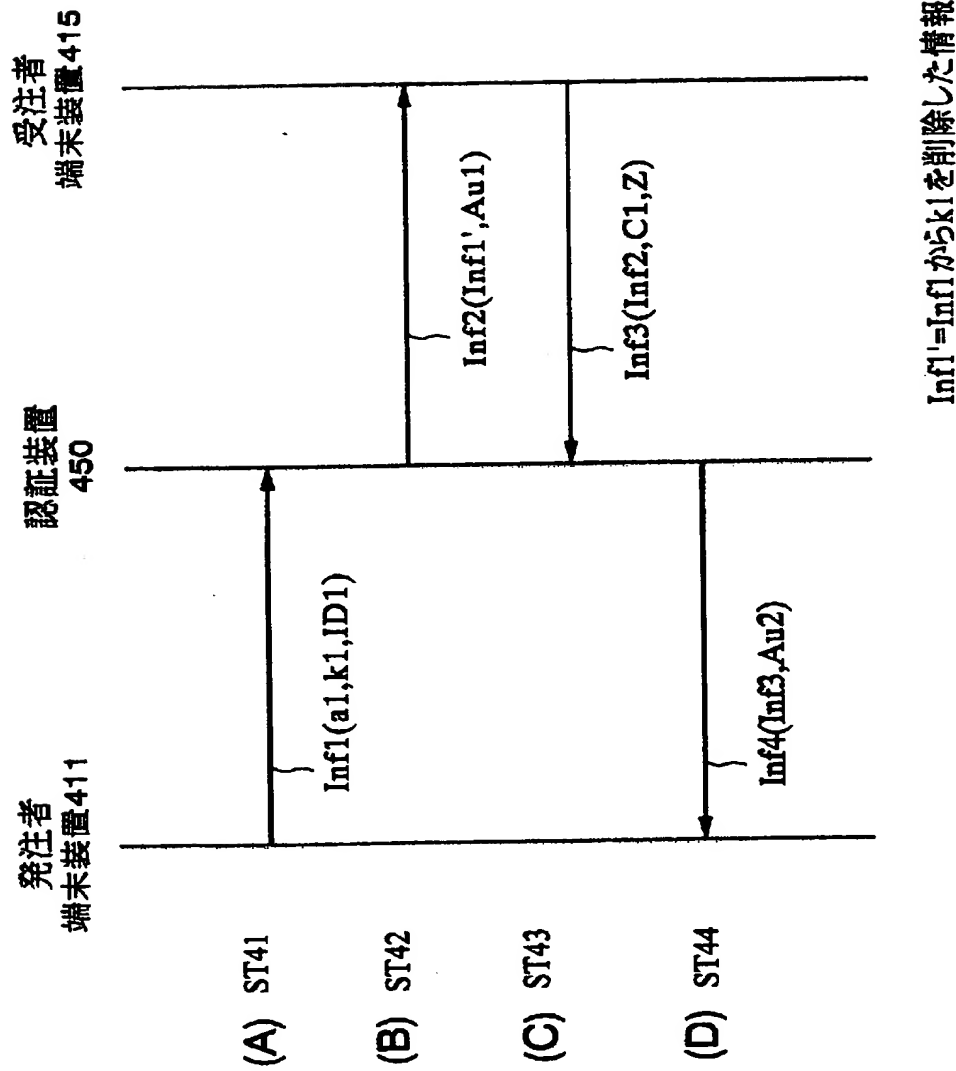
【図 36】



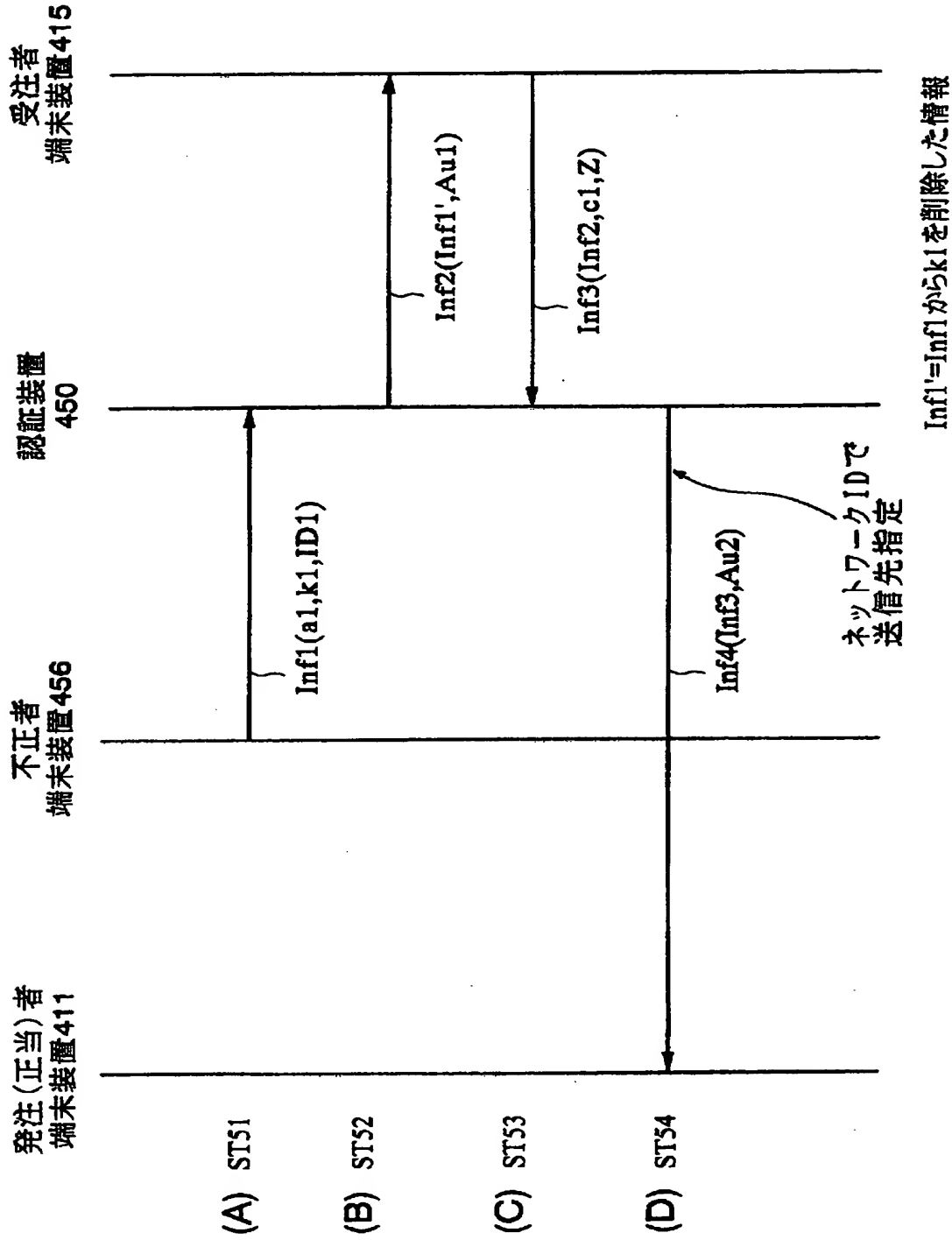
【図 37】



【図 38】

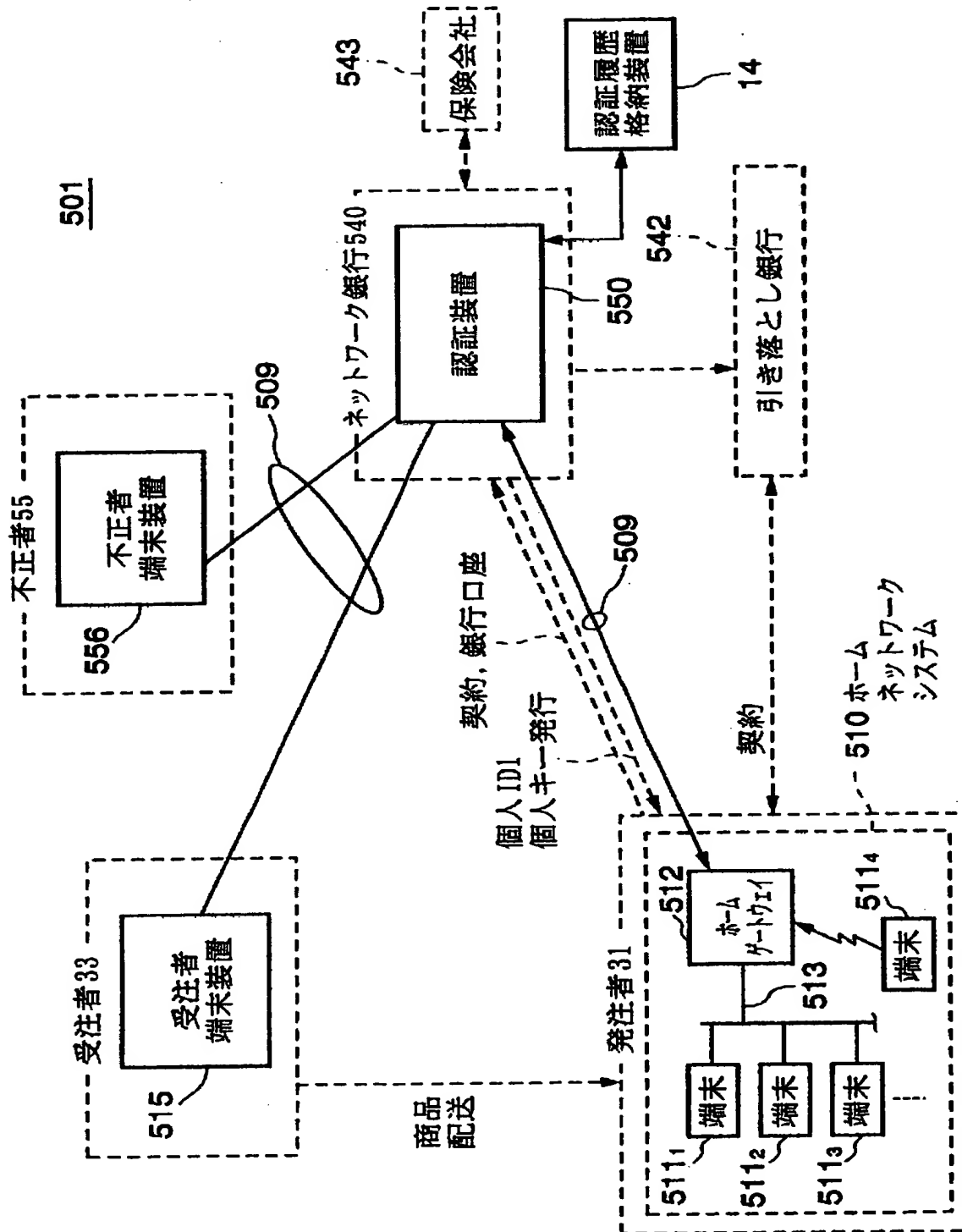


【図 3 9】

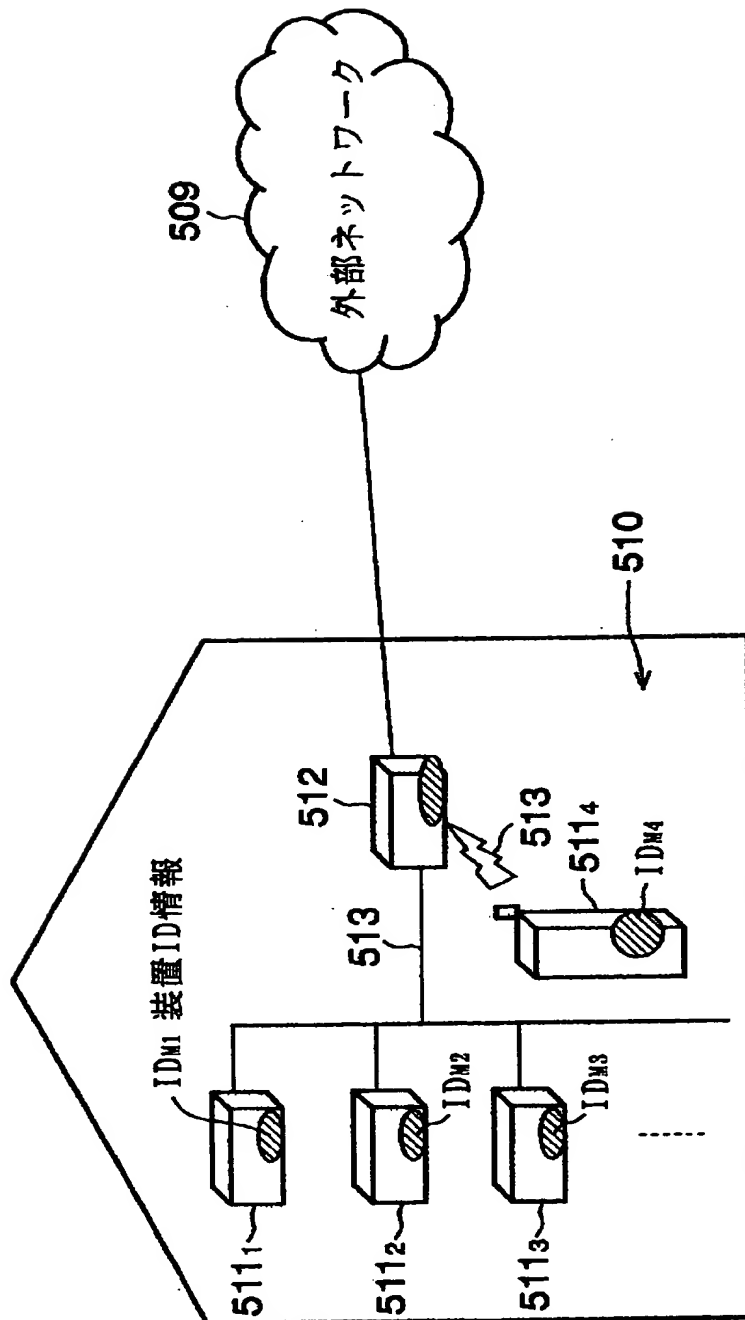




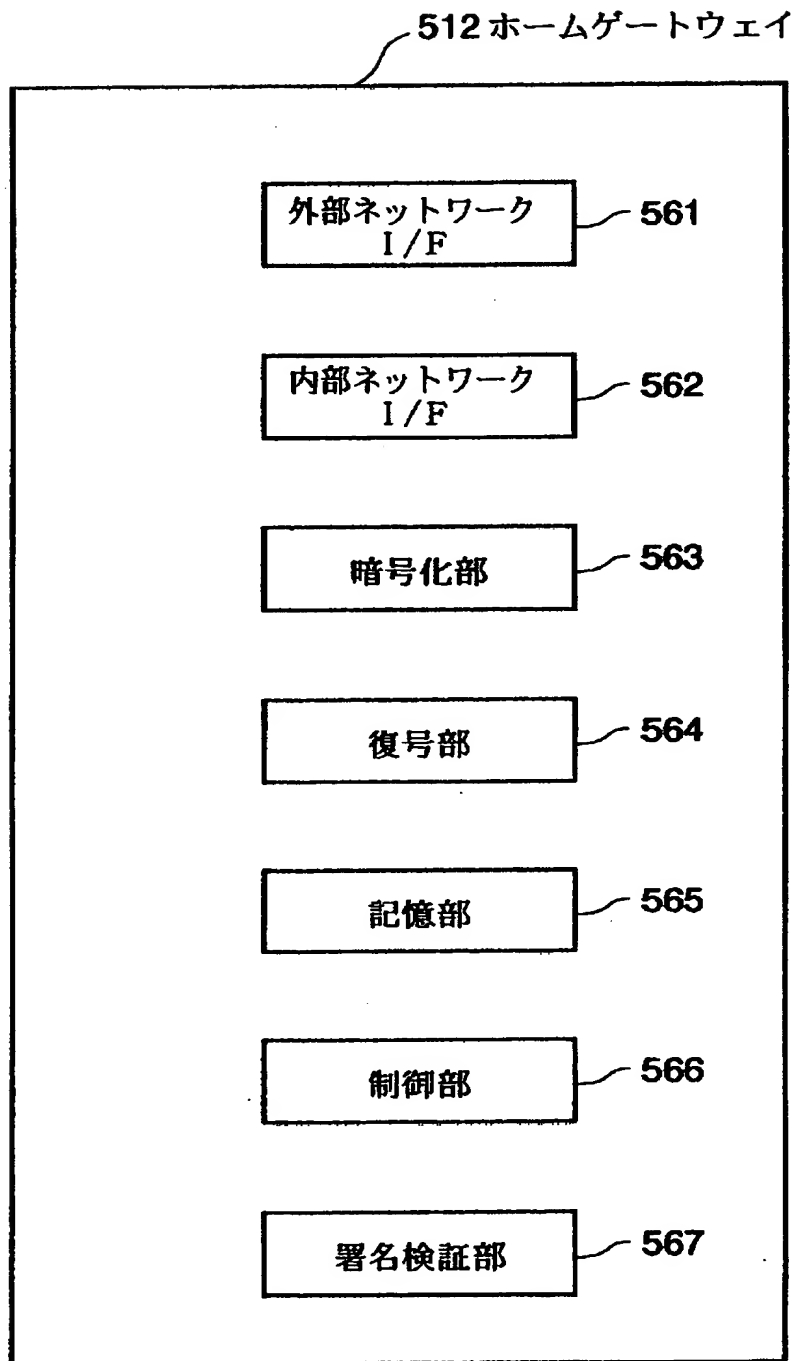
・【図 4 0】



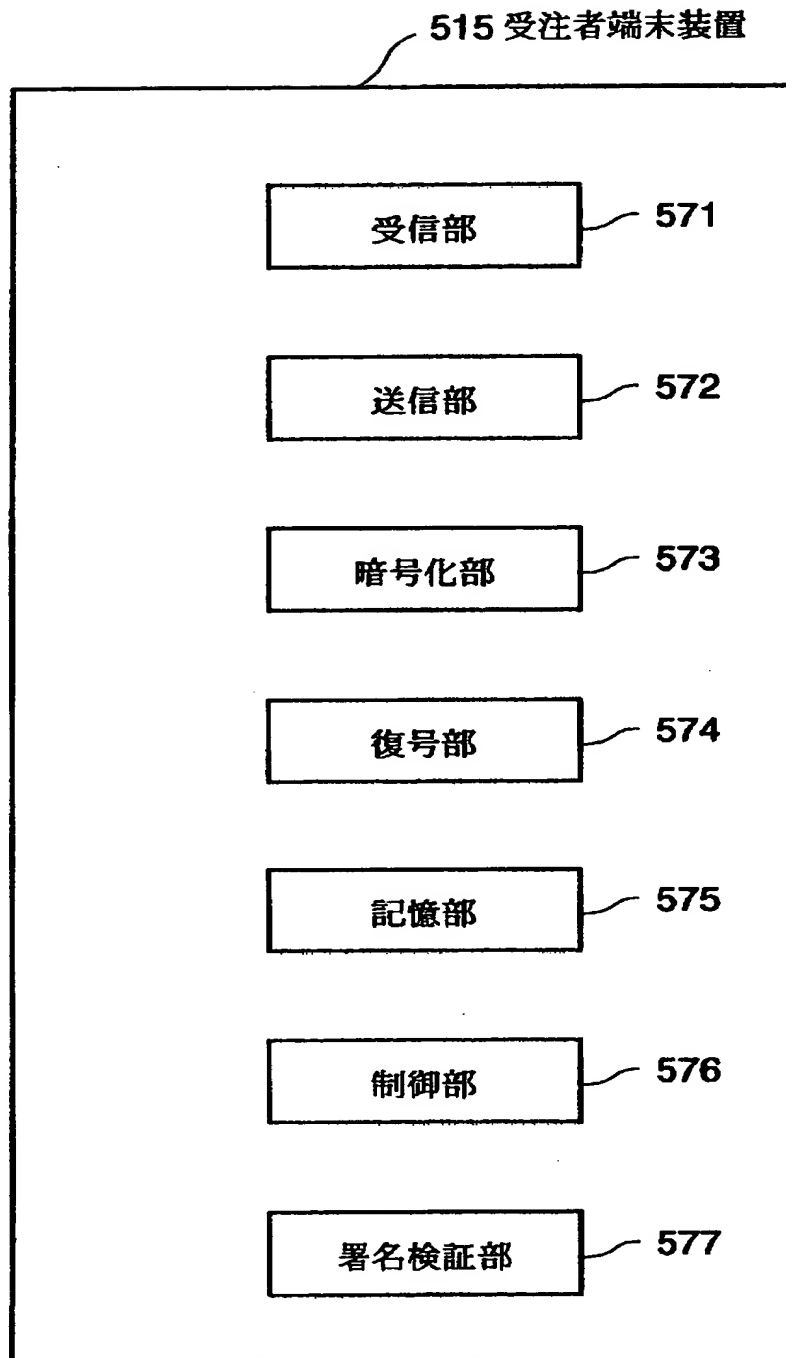
【図 4 1】



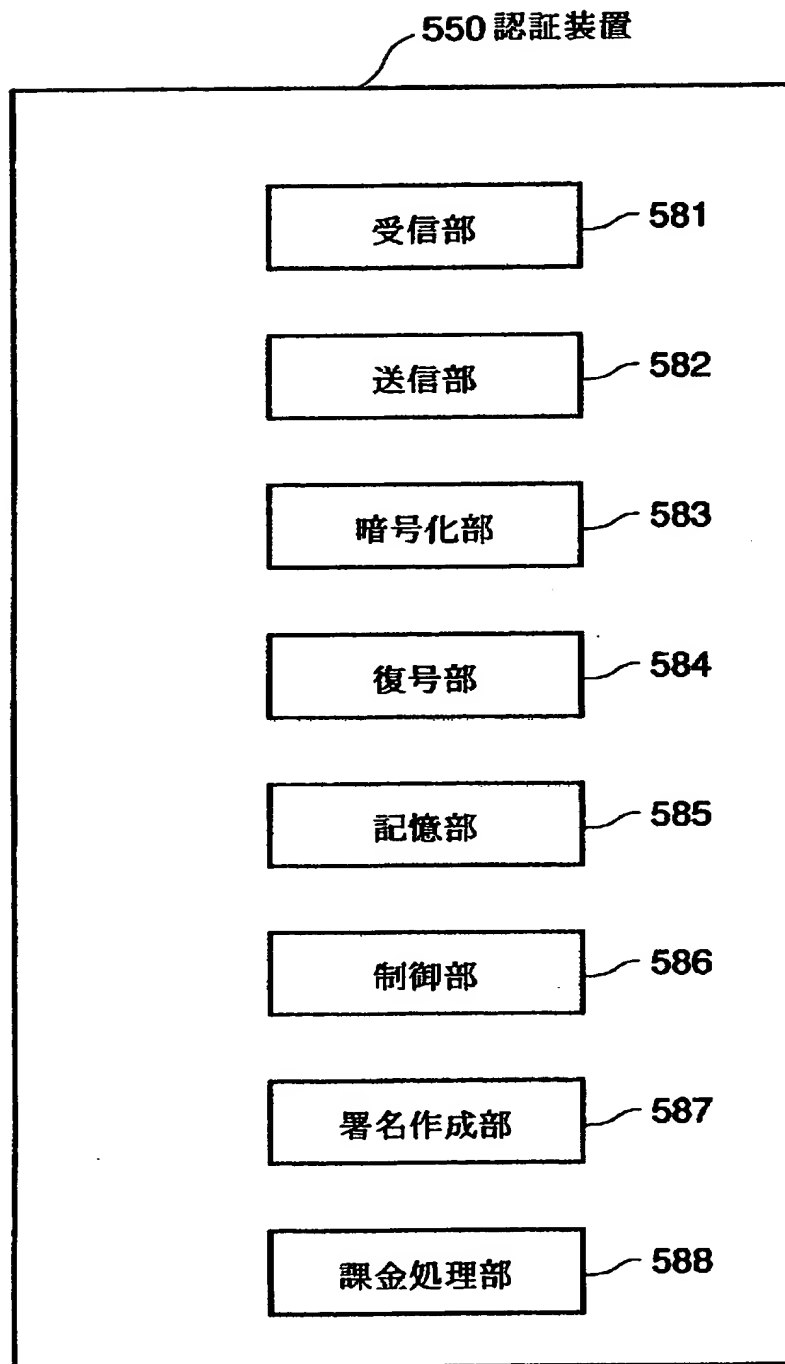
【図 4 2】



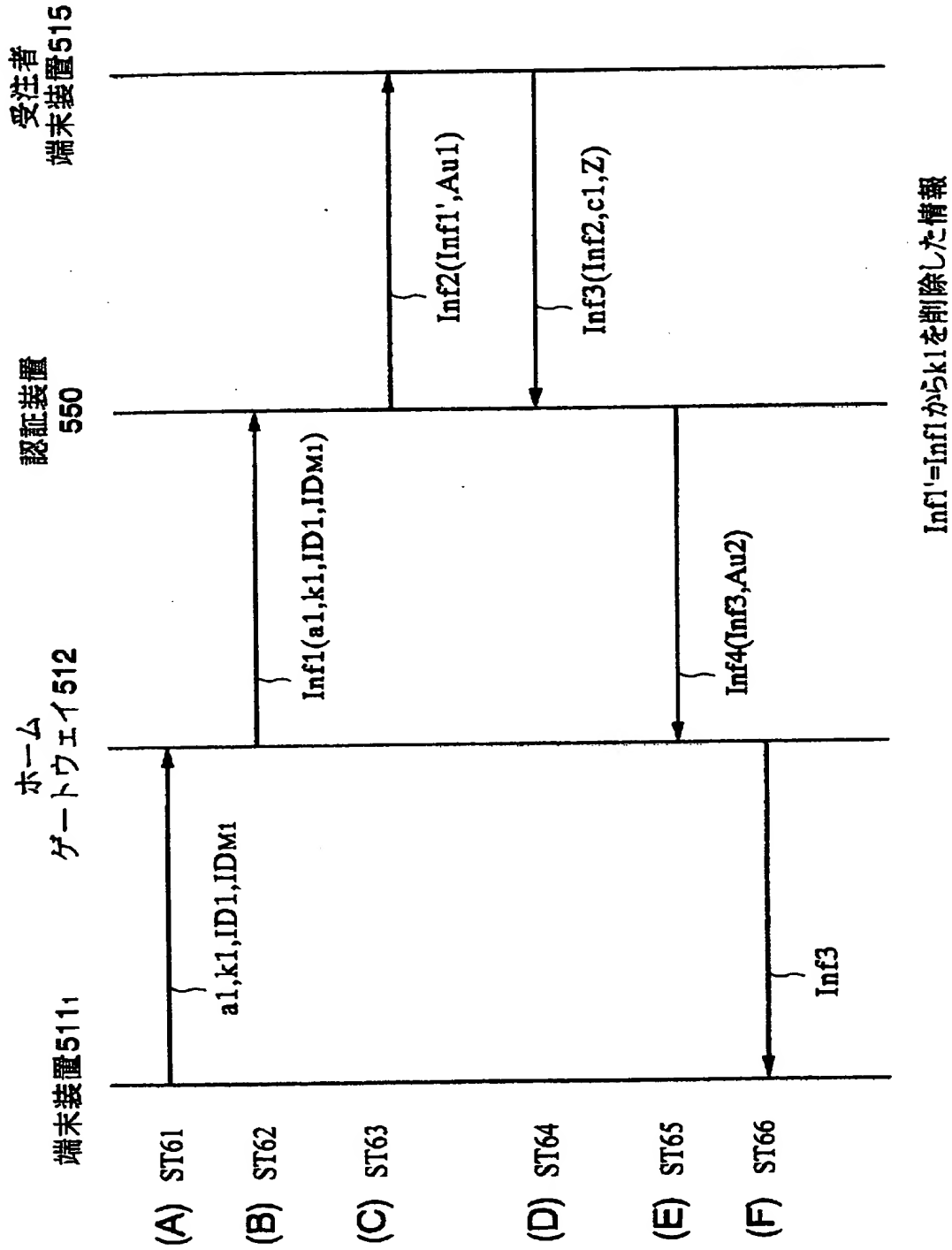
【図43】



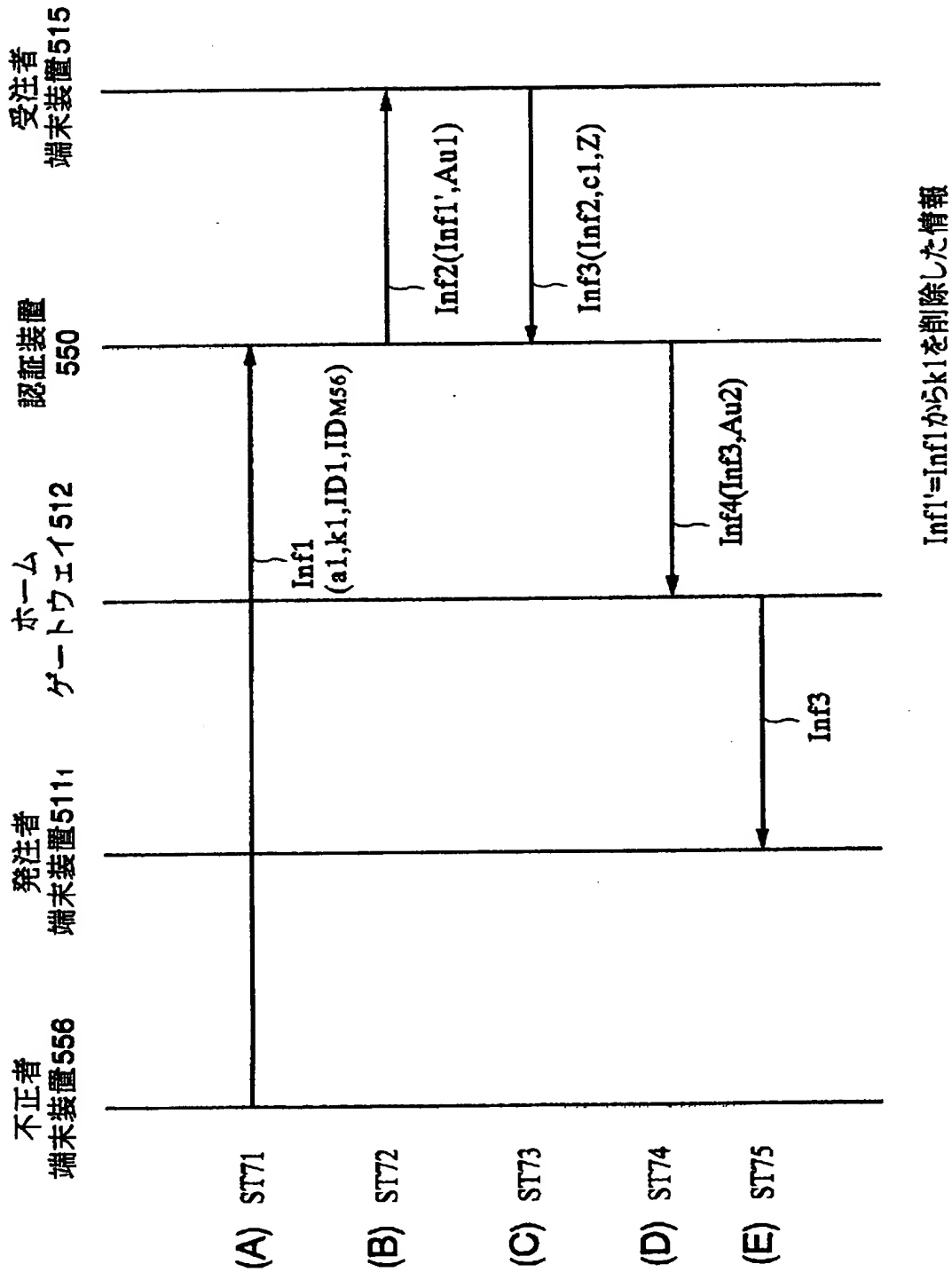
【図 4 4】



【図 45】



【図 46】



【書類名】 要約書

【要約】

【課題】 不正に取得した他人の個人ID情報に基づいて不正な認証手続きが行われることを回避する認証装置を提供する。

【解決手段】 認証装置50は、発注者端末装置11からの認証要求によって、発注者31の個人ID情報ID1と、受注者33の個人ID情報ID2と、取り引き情報とを受信し、受注者端末装置15との間の通信を行った後に、受注者33の正当性を示す認証情報を発注者端末装置11に送信する。

【選択図】 図1



認定・付加情報

特許出願の番号	特願2000-370519
受付番号	50001568808
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年12月 8日

<認定情報・付加情報>

【特許出願人】	
【識別番号】	000002185
【住所又は居所】	東京都品川区北品川6丁目7番35号
【氏名又は名称】	ソニー株式会社
【代理人】	申請人
【識別番号】	100094053
【住所又は居所】	東京都台東区柳橋2丁目4番2号 創進国際特許 事務所
【氏名又は名称】	佐藤 隆久

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社